USER'S MANUAL

AXIS Q1910 Thermal Network Camera

AXIS Q1910-E Thermal Network Camera

Notices

This manual is intended for administrators and users of the AXIS Q1910/Q1910-E Thermal Network Camera, and is applicable for firmware release 5.11 and later. It includes instructions for using and managing the camera on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be beneficial for advanced users, for developing shell scripts and applications. Later versions of this document will be posted to the Axis Website, as required. See also the product's online help, available via the Web-based interface.

Liability

Every care has been taken in the preparation of this manual. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Intellectual Property Rights

Axis Communications AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at http://www.axis.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.

This product contains licensed third-party software. See the menu item "About" in the product's user interface for more information.

This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see http://www.opensource.apple.com/apsl/).
The source code is available from:
http://developer.apple.com/darwin/projects/bonjour/

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

Apple, Boa, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Netscape Navigator, OS/2, Real, SMPTE, QuickTime, UNIX, Windows, WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Axis Communications AB is independent of Sun Microsystems Inc.
UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:

- download user documentation and firmware updates
- find answers to resolved problems in the FAQ database. Search by product, category, or phrases
- report problems to Axis support by logging in to your private support area
- visit Axis Support at www.axis.com/techsup

Safeguards and Warnings

To install the AXIS Q1910/Q1910-E Thermal Network Camera, refer to the Installation Guide supplied with your product.

Caution!

- When transporting the camera, use the original packing or equivalent to prevent damage to the product.
- Avoid exposing the camera to vibration, shocks or heavy pressure and do not install the camera on unstable brackets, unstable or vibrating surfaces or walls, since this could cause damage to the product.
- Only use handtools when installing the camera, the use of electrical tools or excessive force could cause damage to the product.
- Do not aim the camera lens toward the sun or other high-intensity radiation sources since this could cause damage to the sensor.

Important!

- To use AXIS Q1910 outdoors, it must be installed in an approved outdoor housing. Please install AXIS Q1910-E for outdoor use or see www.axis.com for more information on outdoor housing and other accessories.
- The camera should be installed by a trained professional. Please observe relevant national and local regulations for the installation.
- Do not install the camera near heat sources since fluctuating temperatures may affect image quality.
- This product must be used in compliance with local laws and regulations.
- Store and transport the camera in a dry and ventilated environment. Keep the storage and operating temperature between -40°C and 50°C (-40°F and122°F).

Care and maintenance

- Do not use chemicals, caustic agents, or aerosol cleaners. Use a damp cloth for cleaning.
- Only use accessories and replacement parts provided or recommended by Axis.
- Do not attempt to repair the product by yourself, contact Axis or your Axis reseller for service matters.

AXIS Q1910/Q1910-E Thermal Network Camera User's Manual
Rev. 1.0
Copyright© Axis Communications AB, 2009
December 2009 Part no. 36577

Table of contents

Product overview 4
Key features 4
Hardware overview 5
Unit connectors 6
LED indicators 8
Accessing the camera 9
Access from a browser 9
Access from the Internet 10
Setting the root password 10
Video Streams 13
How to stream H.264 13
Motion JPEG 13
Alternative methods of accessing the video stream 14
Setup Tools 15
Basic Setup 15
Video & Audio 16
Video Stream 16
Stream Profiles 18
Camera Settings 18
Overlay Image 18
Privacy Mask 19
Audio Settings 19
Audio Clips 20
Live View Config 21
Layout 21
PTZ (Pan Tilt Zoom) 23
Installing a Pan Tilt device 23
Preset Positions 23
Advanced 23
Control Queue 24
Applications 25
Events 26
Event Servers 26
Event Types 26
Camera tampering 28
Motion Detection 29
Port Status 30
Recording List 31
System Options 32
Security 32
Date & Time 34
Network 34
Storage 39
Ports & Devices 39
LED Settings 39
Maintenance 39
Support 40
Advanced 41
About 41
Resetting to the factory default settings 42
Troubleshooting 43
Checking the firmware 43
Upgrading the firmware 43
Symptoms, possible causes, and remedial action 45
Technical Specifications 48
General performance considerations 50
Index 51

Product overview

This manual applies to the following products:

- AXIS Q1910 Thermal Network Camera (indoor use)
- AXIS Q1910-E Thermal Network Camera (outdoor use)

AXIS Q1910/-E Thermal Network Cameras use thermal imaging technology to detect and convert thermal radiation to images. Thermal radiation, or heat, is a type of electromagnetic radiation emitted by all objects, even by cold objects like ice. Thermal cameras do not require any visible light and can operate in complete darkness and difficult weather conditions such as smoke, haze, dust and light fog.

Images produced by a thermal camera show the temperature variations in the scene. Thermal images are often displayed in bright, intense colors which are created digitally to help the human eye distinguish details in the scene. Each color represents a different temperature; white and red are usually used for higher temperatures, while green, blue and violet are used for colder ones.

AXIS Q1910/-E have all the features of Axis other high-end network video products and can be seamlessly integrated into an existing IP-surveillance system. Due to export regulations for dual-use goods, the frame rate is limited to 8.33 fps.

Standard lenses and housings cannot be used with AXIS Q1910/-E because glass blocks thermal radiation. The AXIS Q1910/-E lens and the window in AXIS Q1910-E are instead made of germanium which allows thermal radiation to pass.

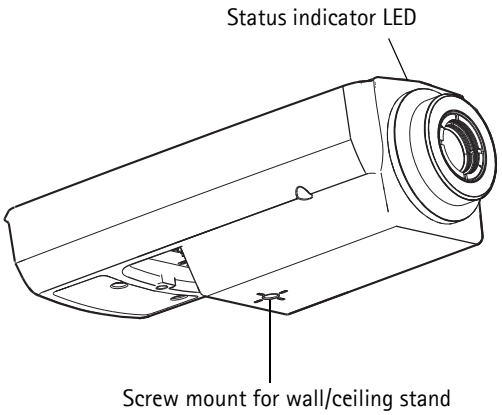
For more information on thermal imaging, please refer to the white paper on thermal cameras available at www.axis.com

Key features

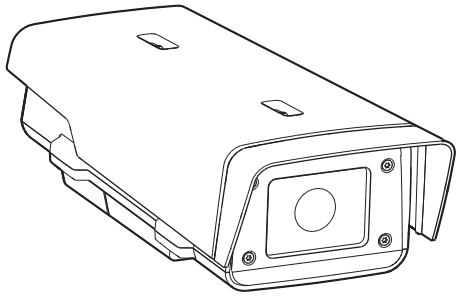
- **Thermal imaging for IP-Surveillance**
  AXIS Q1910/-E offer - for their class - competitive thermal imaging capabilities that allow the user to detect people, objects and incidents in complete darkness and during challenging weather conditions - 24 hours a day, seven days a week.
- **Outdoor-ready model with window heater**
  AXIS Q1910-E is an out-of-the-box, outdoor-ready thermal network camera and comes with a built-in heater for the germanium window. AXIS Q1910 provides auxiliary power for an external heater.
- **Power over Ethernet**
  Power over Ethernet (IEEE 802.3af) supplies power to the cameras via the network, eliminating the need for power cables and reducing installation costs.
- **Multiple H.264 streams with individual palette settings**
  AXIS Q1910/-E are among the first thermal cameras with H.264 support, which provides up to 80% lower bandwidth and storage needs than Motion JPEG. The cameras provide multiple, individually configurable video streams in H.264 and Motion JPEG, and each stream can have its own color palette setting.
- **Intelligent video capabilities**
  AXIS Q1910/-E offer intelligent video capabilities such as video motion detection, audio detection, and detection of tampering attempts. The cameras also provide capacity for third-party analytics modules and AXIS Camera Application Platform.
- **Local storage**
  The cameras come with a built-in slot for an SDHC memory card, enabling storage of more than a month of recordings, without any external equipment.
- **Audio support**
  AXIS Q1910/-E support two-way audio, and are the first thermal cameras with this feature.

Hardware overview

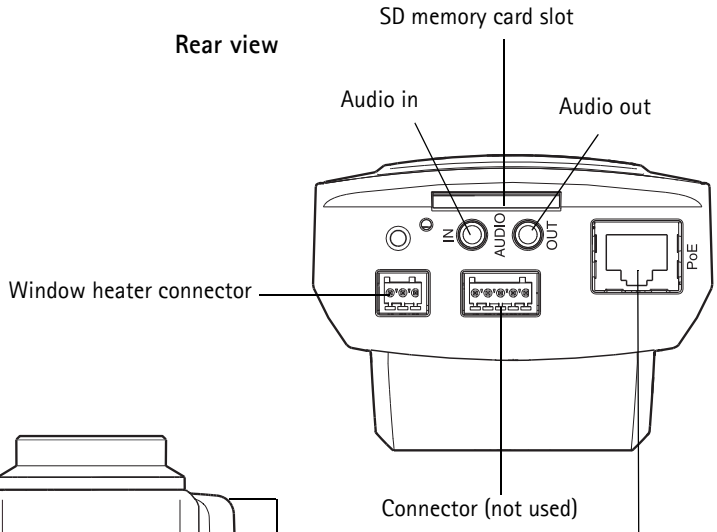
AXIS Q1910



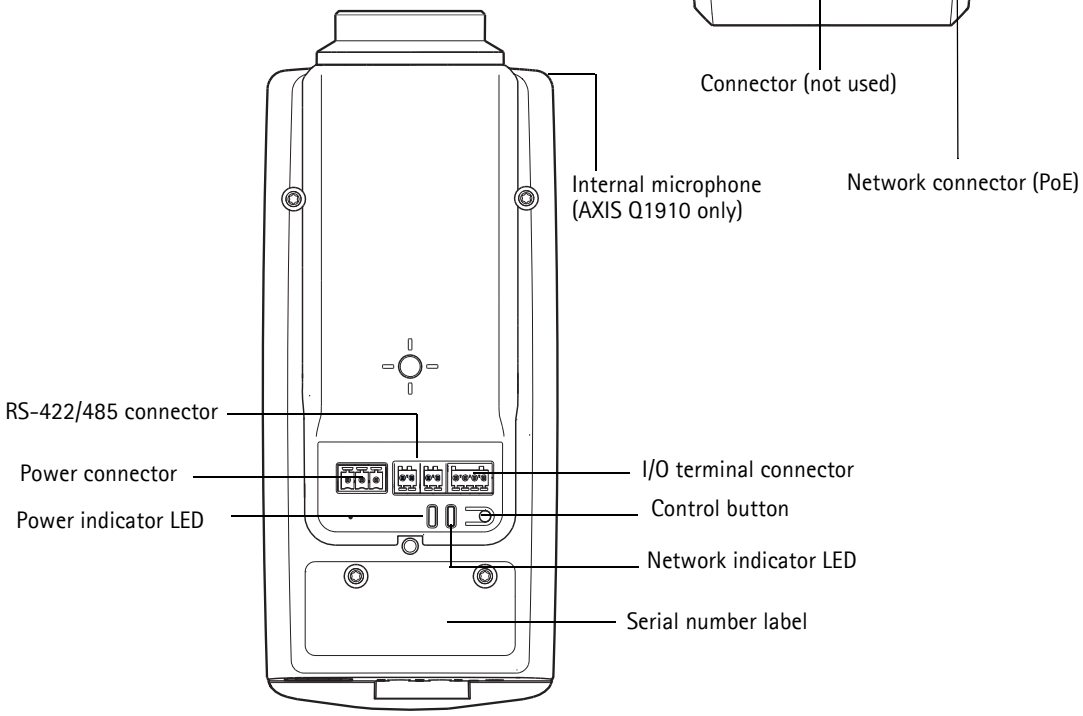
AXIS Q1910-E



Rear view



Bottom view



Unit connectors

Network connector – RJ-45 Ethernet connector. Supports PoE (Power over Ethernet, class 3). Shielded cables should be used to comply with EMC.

Audio in (pink) – 3.5 mm input for a mono microphone, or a line-in mono signal (left channel is used from a stereo signal).

Audio out (green) – 3.5 mm output for audio (line level), can be connected to a public address (PA) system or an active speaker with a built-in amplifier. A pair of headphones can also be connected. A stereo connector must be used for audio out.

SD memory card slot – A standard or high capacity SD memory card (not included) can be used for local recording with removable storage.

Note:

Before removal, the SD card should be unmounted to prevent corruption of recordings. To unmount the SD card, go to **Setup > Systems Options > Storage > SD Card** and click **Unmount**.

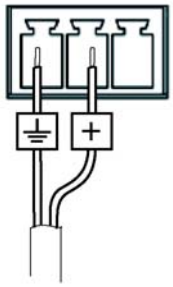
Window heater connector – 3-pin terminal block for connection of the AXIS Q1910-E window heater.

Serial number label – Part number (P/N) and Serial number (S/N). The serial number may be required during installation.

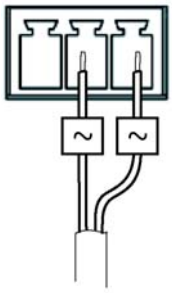
Power connector – 3-pin terminal block for power input. 8-20 V DC, max 11.2 W or 20-24 V AC, max 17.4 VA

Caution!

Incorrect connection of the wires could cause damage to the camera.



DC power input
8 - 20 V DC, max 11.2 W



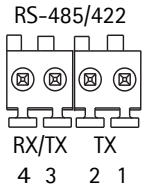
AC power input
20- 24 V AC, max 17.4 VA

Control button – The control button is used for

- Restoring the camera to factory default settings, see *Resetting to the factory default settings,* on page 42.
- Connecting to AXIS Internet Dynamic DNS Service, see page 35. To connect, press the button once.
- Connecting to an AXIS Video Hosting System service, see page 35. To connect, press and hold the button until the Status LED flashes green.

RS-485/422 connector - Two 2-pin terminal blocks for RS-485/422 serial interface used to control auxiliary equipment, e.g. PT devices.

The RS-485/422 serial port can be configured in the following port modes:

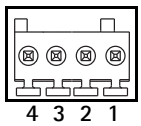


- Bidirectional RS-485 half-duplex port for data transmission using two wires, one combined RX/TX pair.
- Bidirectional RS-485 full-duplex port for data transmission using four wires, one RX pair and one TX pair.
- Unidirectional RS-422 port for transmitting or receiving data using two wires, RX- or TX pair.
- Bidirectional RS-422 full duplex port for data transmission (point-to-point) using four wires, one RX pair and one TX pair

Function	Pin	Notes
RS 485/422TX(A)	1	TX pair for RS-422 and 4-wire RS-485
RS 485/422TX(B)	2	
RS-485A alt RS-485/422RX(A)	3	RX pair for all modes (combined RX/TX for 2-wire RS-485)
RS-485B alt RS-485/422RX(B)	4	

I/O terminal connector

Used in applications for e.g. motion detection, event triggering and alarm notifications. In addition to an auxiliary power and a GND pin, the network camera has 2 pins that can be configured as either input or output. These pins provide the interface to:



- Transistor output - For connecting external devices such as relays and LEDs. Connected devices can be activated by VAPIX® application programming interface (API), by output buttons on the **Live View** page or by an **Event Type**. The output will show as active (shown under **Events > Port Status**) if the alarm device is activated.
- Digital input - An alarm input for connecting devices that can toggle between an open and closed circuit, for example: PIRs, door/window contacts, glass break detectors, etc. When a signal is received the state changes and the input becomes active (shown under **Events > Port Status**.)

Function	Pin	Notes	Specifications
GND	1	Ground	
3.3V DC Power	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	Max load = 250 mA
Configurable (Input or Output)	3 - 4	Digital input - Connect to GND to activate, or leave floating (or unconnected) to deactivate.	Min input = - 40 V DC Max input = + 40 V DC Recommended range: 0 V DC to + 20 V DC
		Digital output - Uses an open-drain NFET transistor with the source connected to GND. If used with an external relay, a diode must be connected in parallel with the load, for protection against voltage transients.	Max load = 100 mA Max voltage = + 40 V DC Recommended voltage: Up to +20 V DC

LED indicators

LED	Color	Indication
Network	Green	Steady for connection to a 100 Mbit/s network. Flashes for network activity.
	Amber	Steady for connection to 10 Mbit/s network. Flashes for network activity.
	Unlit	No network connection.
Status	Green	Steady green for normal operation. Note: The Status LED can be configured to be unlit during normal operation, or to flash only when the camera is accessed. To configure, go to **Setup > System Options > LED.** See the online help files for more information.
	Amber	Steady during startup, during reset to factory default or when restoring settings.
	Red	Slow flash for failed upgrade.
Power	Green	Normal operation.
	Amber	Flashes green/amber during firmware upgrade.

Accessing the camera

To install the AXIS Q1910/-E Thermal Network Camera, refer to the Installation Guide supplied with your product.

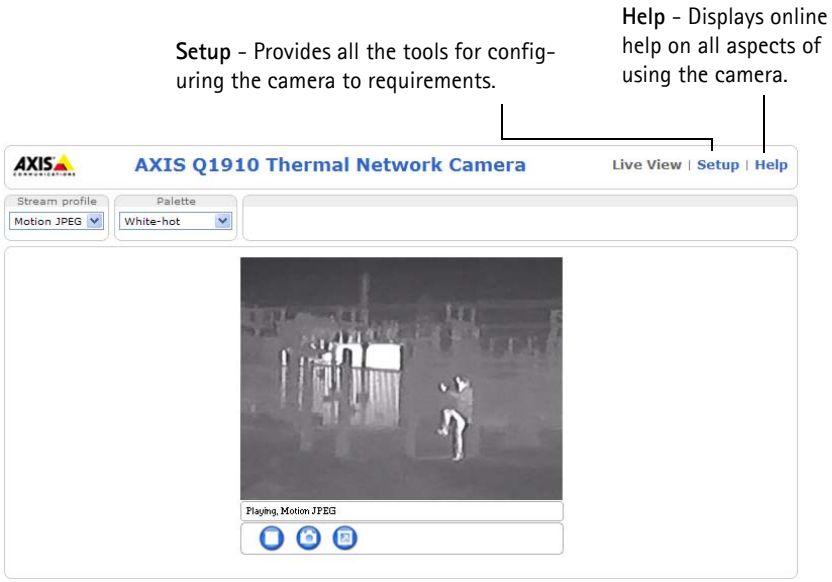
The thermal network camera can be used with most standard operating systems and browsers. The recommended browsers are Internet Explorer with Windows, Safari with Macintosh and Firefox with other operating systems. See *Technical Specifications,* on page 48.

Notes:

- To view streaming video in Internet Explorer, set your browser to allow ActiveX controls and install AXIS Media Control (AMC) on your workstation.
- QuickTime™ is also supported for viewing streaming H.264 video and for audio.
- If your workstation restricts the use of additional software components, the camera can be configured to use a Java applet for viewing Motion JPEG.
- The network camera includes one (1) decoder license for viewing H.264 video streams and one (1) AAC audio license. These are automatically installed with AMC. The administrator can disable the decoder installation, to prevent installation of unlicensed copies.

Access from a browser

1. Start a browser (Internet Explorer, Firefox, Safari).
2. Enter the IP address or host name of the camera in the **Location/Address** field of your browser.
   To access the camera from a Macintosh computer (Mac OSX), click on the Bonjour tab and select your camera from the drop-down list.
3. If this is the first time you are accessing the camera, see *Setting the root password,* on page 10. Otherwise enter your user name and password, set by the administrator.
4. The camera's **Live View** page appears in your browser.


Setup - Provides all the tools for configuring the camera to requirements.
Help - Displays online help on all aspects of using the camera.
AXIS Q1910 Thermal Network Camera
Live View | Setup | Help
Stream profile
Motion JPEG
Palette
White-hot
Playing, Motion JPEG

Note:

The layout of the Live View page may have been customized to specific requirements. Consequently, some of the examples and functions featured here may differ from those displayed on your own Live View page.

Access from the Internet

Once connected, the camera is accessible on your local network (LAN). To access the camera from the Internet you must configure your broadband router to allow incoming data traffic to the camera. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the camera. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.

For more information, please see *NAT traversal (port mapping) for IPv4*, on page 36. See also the AXIS Internet Dynamic DNS Service at www.axiscam.net For Technical notes on this and other topics, visit Axis Support web at www.axis.com/techsup

Setting the root password

To gain access to the product, the password for the default administrator user 'root' must be set. This is done in the **Configure Root Password** dialog, which is displayed when the network camera is accessed for the first time. To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate.

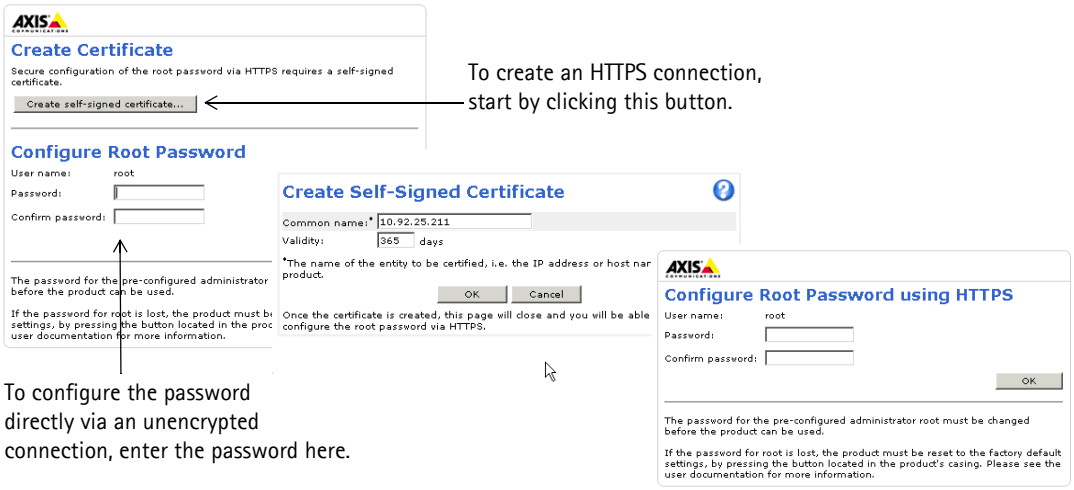
Note:

HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information.

To set the password via a standard HTTP connection, enter it directly in the first dialog shown below.

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click the **Create self-signed certificate** button.
2. Provide the requested information and click **OK**. The certificate is created and the password can now be set securely. All traffic to and from the network camera is encrypted from this point on.
3. Enter a password and then re-enter it to confirm the spelling. Click **OK**. The password has now been configured.


Create Certificate
Secure configuration of the root password via HTTPS requires a self-signed certificate.
Create self-signed certificate...
To create an HTTPS connection, start by clicking this button.
Configure Root Password
User name: root
Password:
Confirm password:
The password for the pre-configured administrator before the product can be used.
If the password for root is lost, the product must be settings, by pressing the button located in the product user documentation for more information.
Create Self-Signed Certificate
Common name: 10.92.25.211
Validity: 365 days
*The name of the entity to be certified, i.e. the IP address or host name product.
OK
Cancel
Once the certificate is created, this page will close and you will be able configure the root password via HTTPS.
Configure Root Password using HTTPS
User name: root
Password:
Confirm password:
OK
The password for the pre-configured administrator root must be changed before the product can be used.
If the password for root is lost, the product must be reset to the factory default settings, by pressing the button located in the product's casing. Please see the user documentation for more information.
To configure the password directly via an unencrypted connection, enter the password here.

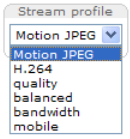
Notes:

- The default administrator user **root** cannot be deleted.
- If the password for root is lost, the network camera must be reset to the factory default settings. See page 42.
- If prompted, click **Yes** to install AXIS Media Control, which allows viewing of the video stream in Internet Explorer. You will need administrator rights on the computer to do this. If using Windows Vista or Windows 7 you must also run Internet Explorer as administrator; right-click the Internet Explorer icon and select **Run as administrator**.
- If required, click the link to install missing decoders.

The Live View page

If your network camera has been customized to meet specific requirements the buttons and other items described below may or may not be displayed on the Live View page. The following provides an overview of each available button.

General controls



The **Stream Profile** drop-down list allows you to select a customized or pre-programmed stream profile on the Live View page. Stream profiles are configured under Video & Audio > Stream Profiles, see *Stream Profiles*, on page 18, for more information.

The **Palette** drop-down list allows you to apply a palette to the image. See *Image Appearance*, on page 16.

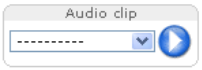
The **Trigger buttons** can trigger an event directly from the Live View page. These are configured under Setup > Live View Config > Layout.

The **Snapshot** button saves a snapshot of the video image currently on display. Right-click on the video image to save it in JPEG format on your computer. This button is primarily intended for use when the AXIS Medial Control viewer toolbar is not available.

The **Output buttons** control the output directly from the Live View page. These buttons are configured under Setup > Live View Config > Layout:

Pulse – Click this button to activate the output for a defined period of time, e.g. switching a light on for 20 seconds.

Active/Inactive – Click these buttons to manually start and stop a connected device, e.g. switch a light on/off.



Audio clips can be played manually from the Live View page. Select the audio clip from the drop-down list and click play.

AXIS Media Control toolbar

The AXIS Media Control viewer toolbar is available in Internet Explorer only. See *AXIS Media Control (AMC)*, on page 14 for more information. The toolbar displays the following buttons:

The **Play** button connects to the product and playing a live video stream.

The **Stop** button stops the live video stream being played.

The **Snapshot** button saves a snapshot of the video image on display. The image is saved in the folder specified in the AMC Control Panel.

Click the **View Full Screen** button to make the video image fill the entire screen area. Press **Esc** (Escape) on the computer keyboard to exit full screen, or right-click and select the option to exit.

The **Record** button is used to start a recording directly from the Live View page. The recording is saved in the folder specified in the Recording tab in the AMC Control Panel.

AMC audio controls

AMC audio buttons control the speakers and microphone connected to the computer. The buttons are only visible when audio is enabled.

Speaker buttons – Click to switch the sound on or off.

Microphone buttons – Click to switch the sound on or off.
In Simplex - Network Camera speaker only mode, click this button to stop sending audio to the camera.

Use the slider to control the **volume** on the speaker and microphone.

Half-duplex mode
The **Talk/Listen button** is used to switch between sending and receiving audio. The button can be configured from the Audio tab in the AMC control panel:

- Push-To-Talk mode: Click and hold the button to talk/send; release the button to listen
- Toggle mode: Click once to switch between talking and listening

Simplex - Thermal Network Camera speaker only mode
To send audio, the Talk and Microphone buttons must both be enabled. Click either button to stop audio transmission.

Video Streams

The network camera provides several image and video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in the network camera provides access to H.264 and Motion JPEG video streams, and to the list of available stream profiles. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

How to stream H.264

This video compression standard makes good use of bandwidth, and can provide high quality video streams at less than 1 Mbit/s.

Deciding which combination of protocols and methods to use depends on your viewing requirements, and on the properties of your network. The available options in AXIS Media Control are:

<table>
<tr><td>Unicast RTP</td><td>This unicast method (RTP over UDP) is used for live unicast video, especially when it is important to always have an up-to-date video stream, even if some images are dropped.</td><td rowspan="3">Unicasting is used for video-on-demand transmission, so that there is no video traffic on the network until a client connects and requests the stream.

Note that there are a maximum of 10 simultaneous unicast connections.</td></tr>
<tr><td>RTP over RTSP</td><td>This unicast method (RTP tunneled over RTSP) is useful as it is relatively simple to configure firewalls to allow RTSP traffic.</td></tr>
<tr><td>RTP over RTSP over HTTP</td><td>This unicast method can be used to traverse firewalls. Firewalls are commonly configured to allow the HTTP protocol, thus allowing RTP to be tunneled.</td></tr>
<tr><td>Multicast RTP</td><td colspan="2">This method (RTP over UDP) should be used for live multicast video. The video stream is always up-to-date, even if some images are dropped.
Multicasting provides the most efficient usage of bandwidth when there are large numbers of clients viewing simultaneously. A multicast cannot however, pass a network router unless the router is configured to allow this. It is not possible to multicast over the Internet, for example.
Note also that all multicast viewers count as one unicast viewer in the maximum total of 10 simultaneous connections.</td></tr>
</table>

AXIS Media Control negotiates with the camera to determine the transport protocol to use. The order of priority, listed in the AMC Control Panel, can be changed and the options disabled, to suit specific requirements.

Important!

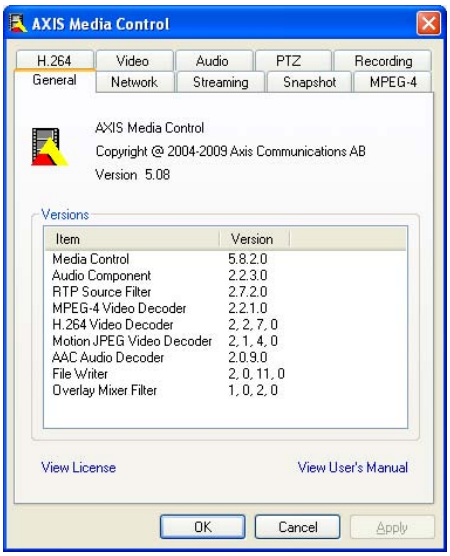
H.264 and AAC are licensed technologies. The network camera includes one H.264 viewing client license and one AAC audio client license. Installing additional unlicensed copies of the clients is prohibited. To purchase additional licenses, contact your Axis reseller.

Motion JPEG

This format uses standard JPEG still images for the video stream. These images are then displayed and updated at a rate sufficient to create a stream that shows constantly updated motion.

The Motion JPEG stream uses considerable amounts of bandwidth, but provides excellent image quality and access to every image contained in the stream. The recommended method of accessing Motion JPEG live video from the network camera is to use the AXIS Media Control (AMC) in Internet Explorer in Windows.

AXIS Media Control (AMC)



The recommended method of accessing live video from the network camera is to use the AXIS Media Control (AMC) in Internet Explorer in Windows.

The AMC Control Panel can be used to configure various video and audio settings. Please see the readme file included in the tool for more information.

The AMC Control Panel is automatically installed on first use, after which it can be configured. Open the AMC Control Panel from:

- Windows Control Panel (from the Start menu)
- Alternatively, right-click the video image in Internet Explorer and click **Settings**

Alternative methods of accessing the video stream

Video/images from the network camera can also be accessed in the following ways:

- Motion JPEG server push (if supported by the client, Firefox, for example). This option maintains an open HTTP connection to the browser and sends data as and when required, for as long as required.
- Still JPEG images in a browser. Enter the path - http://<ip>/axis-cgi/jpg/image.cgi?
- Windows Media Player. This requires AXIS Media Control and the H.264 viewing client to be installed. The paths that can be used are listed below in the order of preference:
  - Unicast via RTP: axrtpu://<ip>/axis-media/media.amp
  - Unicast via RTSP: axrtsp://<ip>/axis-media/media.amp
  - Unicast via RTSP, tunneled via HTTP: axrtsphttp://<ip>/axis-media/media.amp
  - Multicast: axrtpm://<ip>/axis-media/media.amp

<ip> = IP address

- To access the video stream from **QuickTime™** the following paths can be used:
  - rtsp://<ip>/axis-media/media.amp
  - rtsp://<ip>/axis-media/media.3gp

Notes:

- The network camera supports QuickTime 6.5.1 and later
- QuickTime adds latency to the video and audio stream (up to 3 seconds)
- It may be possible to use other players to view the H.264 stream using the paths above, although Axis does not guarantee this
- For input parameters to media.amp, refer to the VAPIX® Application Programming Interface (API) specification.

Accessing audio streams

The Live View page provides access to audio through AXIS Media Control; in addition audio can be accessed in the following ways:

VAPIX®

Audio can be accessed through the VAPIX® application programming interface (API). For more information visit http://www.axis.com/techsup

QuickTime and Windows Media Player

Simplex audio can be accessed via QuickTime and Windows Media Player by using the same paths as for video streams (see above). QuickTime supports G.711 and AAC audio encoding.

Java applet

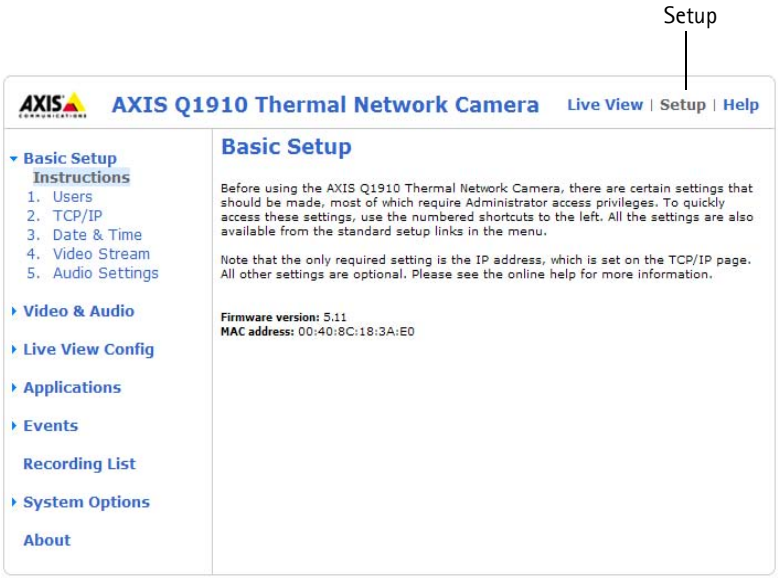
The Java applet supports simplex audio with G.711 encoding.

Setup Tools

The network camera can be configured by users with administrator or operator rights. To access the product's Setup tools, click **Setup** in the top right-hand corner of the Live View page.

- **Administrators** have unrestricted access to all settings
- **Operators** have access to Video & Audio, Live View Config, PTZ, Applications, Events and Recording List

See also the online help available by clicking on each Setup page.


Setup
AXIS Q1910 Thermal Network Camera
Live View | Setup | Help
Basic Setup
Instructions
1. Users
2. TCP/IP
3. Date & Time
4. Video Stream
5. Audio Settings
Video & Audio
Live View Config
Applications
Events
Recording List
System Options
About
Basic Setup
Before using the AXIS Q1910 Thermal Network Camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the numbered shortcuts to the left. All the settings are also available from the standard setup links in the menu.
Note that the only required setting is the IP address, which is set on the TCP/IP page. All other settings are optional. Please see the online help for more information.
Firmware version: 5.11
MAC address: 00:40:8C:18:3A:E0

Basic Setup

Basic Setup provides shortcuts to settings that should be made before using the network camera:

1. Users, see page 32
2. TCP/IP, see page 34
3. Date & Time, see page 34
4. Video Stream, see page 16
5. Audio Settings, see page 19

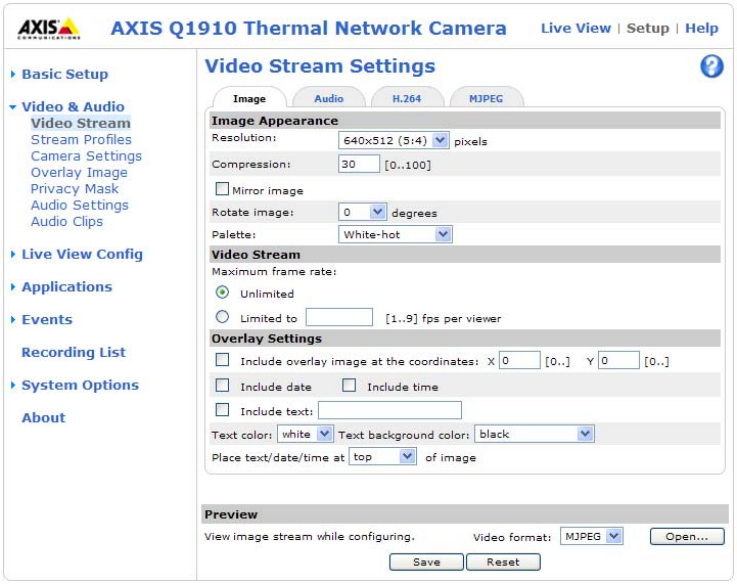
Video & Audio

Click to access the online help that explains the Setup tools.

Video Stream

The video stream settings are in four tabs:

- Image
- Audio
- H.264
- MJPEG



Image

Image Appearance

Use these settings to modify the image **resolution** and **compression**. Setting the compression level affects the image quality and the amount of bandwidth required, the lower the compression, the higher the image quality with higher bandwidth requirements.

The camera is designed to be installed with the logotype facing up but if the installation requires another position, the image can be rotated to the correct orientation. Select the appropriate value from the drop-down list. The image can also be mirrored (reversed).

The image can be colored by applying a **palette**. Colors in the image indicate temperature differences and can be used to improve visibility of fine details. The palette selected here is used as the default palette, other palettes can be selected on the Live View page.

Video Stream

To avoid bandwidth problems on the network, the **frame rate** allowed to each viewer can be limited. Select the **Unlimited** radio button to allow the highest available frame rate or select the **Limited to...** radio button and enter a value in the field.

Overlay Settings

To place an overlay image at specific coordinates in the live view image, check the **Include overlay image at the coordinates** box and enter the X and Y coordinates. The overlay image must first be uploaded to the camera, see *Overlay Image*, on page 18.

Text, date and time can also be used as an overlay. Click for information on available options.

Preview

For a preview of the image before saving, select video format and **Open**. When satisfied with the settings, click **Save**.

Text, date and time overlay

Audio

Enable Audio

Check the **Enable audio** box to enable audio in the video stream.

The Audio configuration settings are the same for all video streams and configured under **Video & Audio > Audio Settings**, see page 19. The current audio configuration is displayed under **Current Audio Settings**.

Note:

The checkbox **Enable Audio Support** on the **System Options > Security > Audio Support** must also be checked to enable sound in the product. See *Audio Support,* on page 33**.**

H.264

GOV Settings

The GOV structure describes the composition of the video stream and setting the GOV-length to a higher value saves considerably on bandwidth but may have an adverse effect on image quality.

Bit Rate Control

The bit rate can be set as **Variable Bit Rate** (VBR) or **Constant Bit Rate** (CBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area.

CBR allows you to set a fixed **Target bit rate** that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either frame rate or image quality. Not setting a priority means frame rate and image quality are equally affected.

Note:

To determine a reasonable bit rate, go to **Setup > Video & Audio > Video Stream > Image**. Under Overlay Settings, check the **Include text** checkbox and enter the code **#b** in the field. The current bit rate will display as a text overlay on the Live View page.

To view the image stream while configuring the GOV settings and Bit rate control, select **Open...** under **Preview.**

MJPEG

Frame Size Control

To control the bandwidth and storage used by the Motion JPEG video stream the maximum frame size can be limited. The Default option provides consistently good image quality at the expense of increased bandwidth and storage usage whenever image activity increases. To prevent increased bandwidth and storage usage, set the maximum frame size to a fixed value.

Stream Profiles

Pre-programmed stream profiles are available for quick set-up. These settings can be adjusted and new, customized profiles can be created. Each profile has a descriptive name, describing its usage and/or purpose. The profiles can be accessed from the Live View page.

- To create a new stream profile, click **Add** to bring up the **Stream Profile Settings** dialog.
  1. Enter a unique name and a description for the profile.
  2. Select a **Video encoding** (H.264 or MJPEG) from the drop-down list.
  3. Modify the stream settings under the **Image**, **Audio**, **H.264** and **MJPEG** tabs. See *Video Stream*, on page 16**.**
  4. Click **OK** to save the profile.
- To copy and existing stream profile, click **Copy...** and enter a new name, Change the stream profile settings as above.
- Choose the form of **Video encoding** you wish to use from the drop-down list:
- To modify an existing stream profile, click **Modify...** and change the settings as above. The original settings for the pre-programmed profiles can always be restored by clicking **Restore.**
- To remove a stream profile, click **Remove**. Pre-programmed profiles cannot be removed.

Camera Settings

This page provides access to the image settings for the network camera.

Image Appearance

Brightness – The image brightness can be adjusted in the range 0-100, where a higher value produces a brighter image.

Contrast – Adjust the image's contrast by raising or lowering the value in this field.

Exposure Settings

Configure the exposure settings to suit the image quality requirements in relation to temperature variations in the scene.

Exposure control – This setting is used to adapt to the amount of thermal radiation. For most situations, the **Automatic** setting can be used.

Exposure zones – This setting determines which part of the image is used to calculate the exposure. For most situations, the **Auto** setting can be used, but for particular requirements, check **Defined** and then click **Edit...** and select one of the predefined areas.

Gain – This setting controls the gain. Lowering the gain reduces image noise but can result in a darker image.

Once satisfied, click **Save.** Click **View...** to view the video stream with the current configuration.

Please see the online help files for a description of each available setting.

Overlay Image

An overlay image is a static image superimposed over the video image. The overlay image can be used to provide extra information, or to mask a part of the video image. See the online help for supported image formats and sizes.

To use your own image, e.g. a logo, it must first be uploaded to the network camera. Click **Browse** and locate the image file on the computer. Click **Upload**. When uploaded, the file can be selected in the **Use overlay image** drop-down list.

To place the overlay image at specific coordinates in the live view image, the box **Include overlay image at the coordinates** under **Video & Audio > Video Stream > Image** must be checked, see *Overlay Settings*, on page 16.

Once satisfied, click **Save.**

Privacy Mask

A privacy mask is an area of solid color that prohibits users from viewing parts of the monitored area. Up to three privacy masks can be used. Privacy masks cannot be bypassed via the VAPIX® Application Programming Interface (API).

Privacy Mask List

The Privacy Mask List shows all masks that are currently configured and if they are enabled.

Add/Edit Mask

To define a new mask:

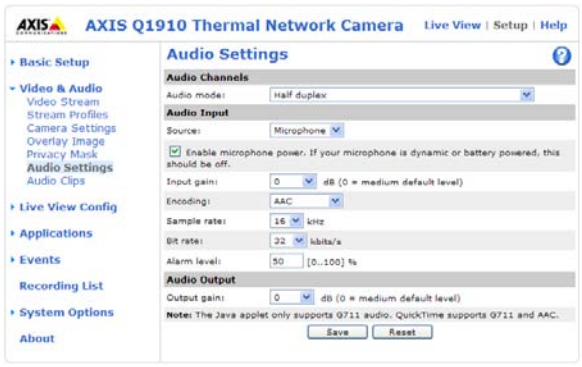
1. Click **Add**. A rectangle appears on the image.
2. Use the mouse to move the rectangle over the area to be concealed. To resize, click and pull the bottom right-hand corner.
3. Enter a descriptive name in Mask name field.
4. Click **Save**.

To edit a privacy mask, select the mask and reshape or move as needed.

To change the **Privacy mask color**, select the a new color from the drop-down list.

Audio Settings

This section describes how to configure the basic audio settings for the network camera. The audio functionality for each video stream is enabled under **Video & Audio > Video Stream > Audio.**



Audio Channels

Audio mode - The available audio modes are:

- **Half duplex**. Audio is transmitted in both directions between the network camera and the client computer, but only in one direction at a time. You must actively transmit/receive sound using the **Talk/Listen** button available on the Live View page (see *AXIS Media Control toolbar*, on page 11). In Push-To-Talk mode, click and hold the button to speak and release it when finished speaking. In Toggle mode, click once to switch between speaking and listening.

  Note: The Talk/Listen button is configured from the Audio tab in the AMC Control panel (see *AXIS Media Control (AMC)*, on page 14).
- **Simplex – Thermal Network Camera speaker only**. Audio is transmitted from the client to the camera and played by the speakers connected to the camera. To send audio, the **Talk** and **Microphone** buttons in the AMC toolbar must both be enabled. Click either button to stop audio transmission.
- **Simplex – Thermal Network Camera microphone only**. Audio captured by the microphone connected to the camera is transmitted from the camera to one or more clients.

Audio Input

An external microphone or a line source can be connected to the Audio in connector. Set **Source** to **Microphone** or **Line** depending on the connected device.

Notes:

- AXIS Q1910 has an internal microphone. If an external microphone or line source has been connected, the internal microphone will be automatically disconnected.
- To prevent unauthorized listening, disable the internal microphone by inserting a plug in the Audio in connector.

The **Enable microphone power** option provides DC power for an external microphone. If using a small electret condenser microphone such as a clip-on microphone or a PC microphone, enable this option.

Notes:

- If **Enable microphone power** is unchecked (disabled), the internal microphone is also disabled.
- To use a high impedance dynamic microphone, do not enable DC power. DC power will not harm the microphone; if you are uncertain, try switching it off and on. The default value is DC power enabled. To use a professional microphone requiring 48V phantom power, you need an external power supply and a balanced-unbalanced converter (audio transformer) in between.

If the sound input is too low or too high, adjust the **input gain** for the microphone attached to the network camera.

Select the desired audio **Encoding** format, G711 µ-law, G726 or AAC.

Select the required **Sample rate** (number of times per second the sound is sampled). The higher the sample rate, the better the audio quality and the greater the bandwidth required.

Changing the **Bit rate** affects the audio compression level and hence audio quality. A higher bit rate can improve audio quality but requires more bandwidth.

The network camera can be configured to trigger an event if the incoming sound level rises above, falls below, or passes the set **Alarm level**.

Audio Output

If the sound from the speaker is too low or too high, adjust the **output gain** for the active speaker attached to the network camera.

Note:

To receive synchronized video in H.264 and audio, it is recommended that the time settings in the camera and client computer are synchronized with an NTP Server. This is enabled in the camera under **System Options > Date & Time**. Please refer to the help pages for more information.

Audio Clips

An audio clip is a sound file that can be played when an event occurs or manually from the Live View page. Audio clips can be uploaded to the camera or recorded using camera's microphone.

Add a new audio clip

To add a new audio clip, click **Add...** The dialog expands with three choices **Record**, **Upload** and **Location**.

Record

To record a new clip using the microphone:

1. Select the **Record** radio button.
2. Enter a descriptive **Name**.
3. If the recording should not start immediately upon clicking the Record... button, enter the number of seconds to wait before recording actually starts.
4. Enter the number of seconds to record.
5. Click **Record...** to start the recording. Once started the recording cannot be aborted.

Notes:

- The Status indicator flashes amber while waiting to record and flashes red while recording.
- If audio quality is not satisfactory, try adjusting the Input gain under Audio Settings.
- Recording time is limited to 60 seconds.

Upload a sound file

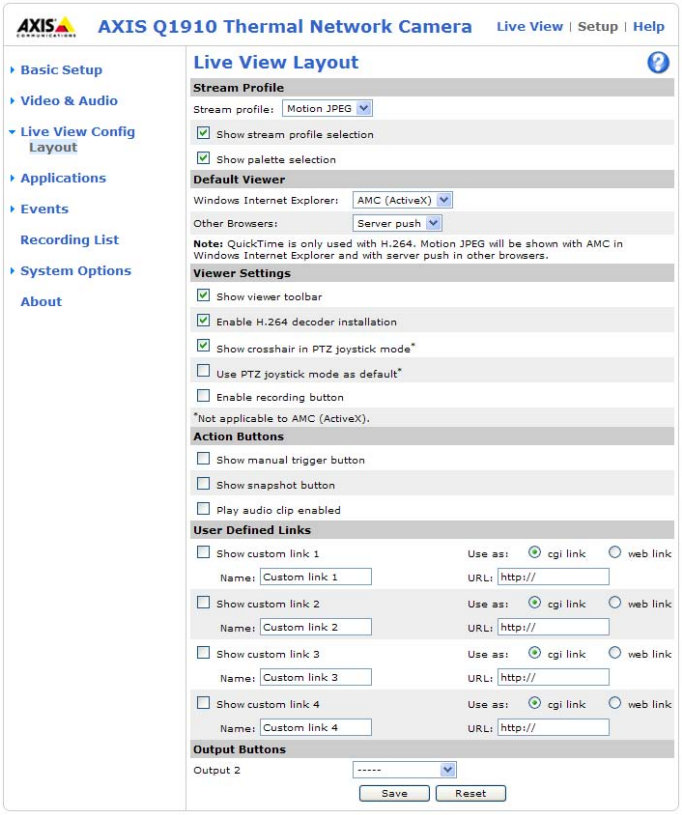
To upload a clip from a local hard drive or network disk, select the **Upload** radio button. Enter a descriptive name, click the **Browse** button and navigate to the desired file. Click **Upload**.

To specify a clip location, select the **Location** radio button and enter the **Name** and location under **Location**. Click **Add clip**.

Live View Config

Layout

The settings on this page are used to customize the appearance of the Live View page.



Stream Profile

From the **Stream Profile** drop-down list, select the stream profile that is to be used for the Live View page. Listed are the pre-programmed stream profiles as well as the ones created under **Video & Audio > Stream Profiles**.

Disable **Show stream profile selection** and **Show palette selection** to remove the Stream Profile and Palette drop-down lists from the Live View page.

Default Viewer

From the drop-down lists, select the default method for viewing video images for your browser. The camera attempts to show the video images in the selected video format and viewer. If this is not possible, the camera overrides the settings and selects the best available combination.

Browser	Viewer	Description
Windows Internet Explorer	AMC	Recommended viewer in Internet Explorer (H.264/Motion JPEG)
	QuickTime	H.264
	Java applet	A slower imaging alternative to AMC. Requires one of the following installed on the client: • JVM (J2SE) 1.4.2 or higher • JRE (J2SE) 5.0 or higher
	Still image	Displays still images only. Hit the Refresh button in your browser to view a new image.
Other browsers	Server Push	Recommended viewer for other browsers (Motion JPEG only)
	QuickTime	H.264
	Java applet	A slower imaging alternative to Server Push (Motion JPEG only)
	Still image	Displays still images only. Hit the Refresh button in your browser to view a new image.

Viewer Settings

Check **Show viewer toolbar** to display the AXIS Media Control (AMC) or the QuickTime viewer toolbar under the video image in your browser.

The administrator can disable the installation of the **H.264 decoder** included with AMC. This is used to prevent the installation of unlicensed copies. Further decoder licenses can be purchased from your Axis reseller.

Enable **Show crosshair in PTZ joystick mode** and a crosshair will indicate the center of the image in PTZ joystick mode.

Check **Use PTZ joystick mode as default** to use joystick mode. The mode can be changed temporarily from the PTZ control panel.

Check the **Enable recording button** to enable recording from the Live View page. The recordings are saved to the location specified in the AMC Control Panel, see *AXIS Media Control (AMC)*, on page 14.

Action Buttons

Check the boxes to display action buttons on the Live View page.

The **manual trigger** button can be used to manually trigger and stop an event. See *Applications*, on page 25.

The **snapshot** button can be used to save a snapshot from the video stream. This button is mainly intended for use with browsers other than Internet Explorer, or when not using AXIS Media Control (AMC) to view the video stream. AXIS Media Control for Internet Explorer has its own snapshot button.

Check **Play audio clip enabled** to display the Audio clip drop-down list, allowing users to manually play audio clips from the Live View page.

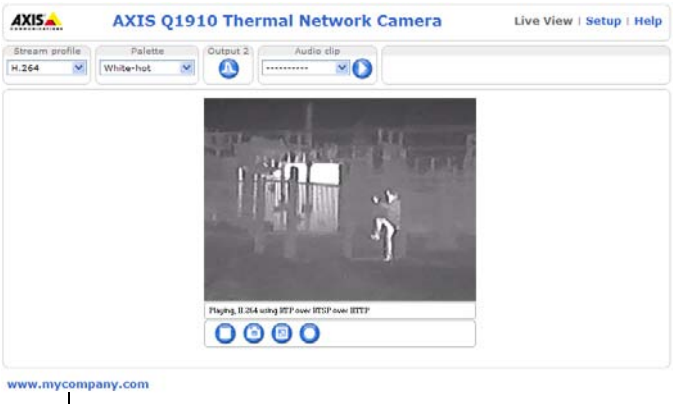
User Defined Links

User-defined links can link to web pages or can be used to run scripts or activate and control external devices connected to the network camera. Once configured, the links appear on the Live View page.

To set up a link, check the **Show custom link** box, select the cgi or web link radio button, enter the URL and a descriptive name in the provided fields.

A link defined as a web link will open in a new window, while a cgi link will run for example a script in the background.

User-defined cgi links can be used to issue API requests. For information on the VAPIX® Application Programming Interface (API), see the Developer pages at Axis web site www.axis.com/developer.



User-defined link

Output Buttons

The output buttons are used to manually activate and inactivate devices connected to the output ports, for example to switch a light on and off. To display output buttons on the Live View page, select the type of control to use for the port from the drop-down list:

- **Pulse** - Activates the output for a defined period of time
- **Active/Inactive** - Displays two buttons, on for each action (on/off)

The camera's I/O ports can be configured as input or output under **System Options > Ports & Devices > I/O Ports**. See *I/O Ports*, on page 39.

PTZ (Pan Tilt Zoom)

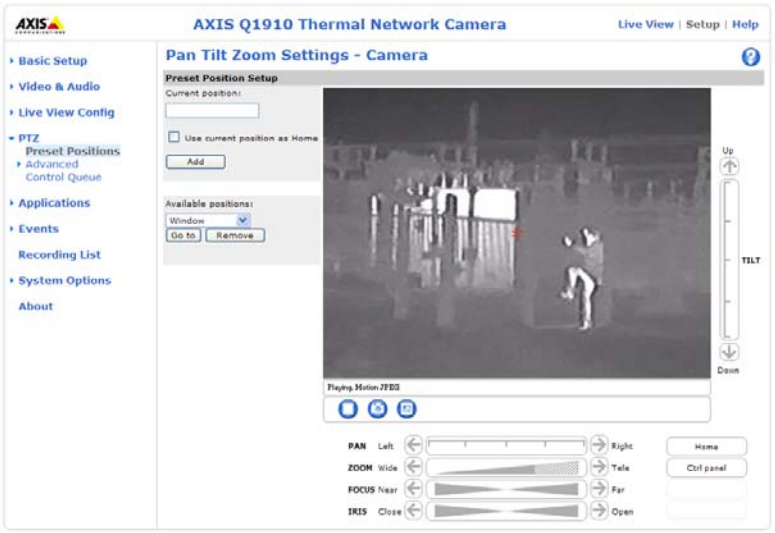
Installing a Pan Tilt device

The network camera can be placed in a P/T device, in order to enable Pan/Tilt control from the camera. See www.axis.com for a list of compatible devices. To install a Pan Tilt device follow these instructions:

1. Connect the Pan Tilt device to the RS-485/422 connector. See *Unit connectors*, on page 6.
2. Go to **Setup > System Options > Ports & Devices > COM Port** and select the appropriate port mode, RS-485 2-wire, RS-485 4 wire or RS-422 2/4-wire.
3. Select **Pan Tilt Zoom** from the **Usage** drop-down list. Click **Apply**.
4. Under **PTZ Driver Management**, click **Upload** to install a PTZ driver. A new window is opened. Click **Browse** and locate the driver in the file system. Click **Upload**.
5. Optionally, click **Port Options** to modify the port settings.
6. Check the box **Video 1** and click **Apply**.

Drivers can be downloaded from www.axis.com

Once PTZ has been installed, PTZ appears in the menu to the left and PTZ controls become available on the Live View page.



Preset Positions

A preset position is a pre-defined camera view that can quickly and easily be accessed.

From **Preset Position Setup**, use the (Pan/Tilt) Zoom control to zoom in to the required position. When satisfied with the camera's position, enter a descriptive name. Click **Add** to save the camera's view as a preset position.

The camera will take the exact position when the preset's name is selected from the Preset position's drop-down list. Preset positions can be selected in **Live View**, and in **events**.

One position can be set as the **Home** position, which is readily accessible by clicking on the **Home** button in both the Preset Position Setup window and the Live View window. The position's name will have (H) added, for example, Entrance (H).

Advanced

Device

Available settings depend on the connected PT unit and uploaded driver, please refer to the online help files and to the documentation provided with the PT unit and driver.

Controls

Panel Shortcut Command Buttons – Here are the controls for creating and saving shortcut command buttons. These buttons can provide direct access to various built-in auxiliary commands provided by the PT driver. The buttons are displayed in the Control Panel, which is available on the Live View page by clicking the **Ctrl panel** button.

Enable/Disable controls – Enable or disable the PTZ by checking/unchecking these boxes. When disabled, the Pan and Tilt sliders will not be available on the Live View page or any other page with the video stream included.

OSD Menu

If the PT unit supports an internal configuration menu, the menu can be accessed using the On-Screen Display (OSD). Configure the PT unit by opening and navigating through the internal menu.

Control Queue

The PTZ Control Queue is a system for placing PTZ control requests in a queue. The control queue fields on the Live View page show the user's current status and position in the queue and the amount of time remaining until PTZ control is given, or if the user already has control - the amount of control time remaining.

Control Queue Settings

Enable PTZ Control Queue – This enables the queuing function and displays the user's status and position in the queue on the Live View page.

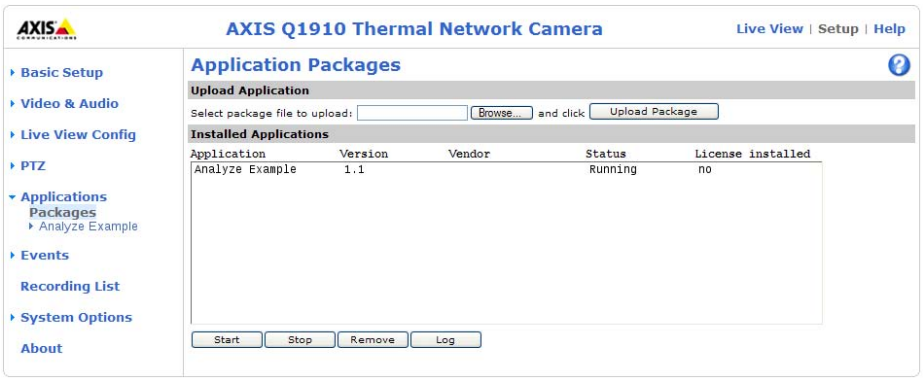
Limit number of users in queue to – This can be specified up to 100. The default value is 20.

Control queue poll time – To keep the control queue up-to-date, the waiting clients must regularly poll the camera to keep their place in the queue. If the client does not send a new poll query within the time set here (in seconds), the client will be dropped from the queue.

Setting a higher value can lead to greater numbers of 'dead' requests in the queue, i.e. when clients leave the queue. Setting too low a value, so that clients are required to send frequent poll queries, may result in the camera becoming overloaded.

Click **Save** to save the settings.

Applications



The Applications feature allows you to upload third-party applications for use on this device. Listed under **Setup > Applications > Packages** are the applications that have already been installed. Click on the name to view the menu options – Settings, License and About.

Settings – Application-specific settings

License – Some applications require a license. If there is an Internet connection **Automatic Installation** appears on the web page. If there is no Internet connection, visit www.axis.com from another computer to acquire a License key file. To receive the license key, you will need a license code and the camera's serial number (found on the product's label, see page 5).

About – Details about the installed application.

Upload Applications

To upload an application, browse to the package and click **Upload Package**.

Installed Applications

Uploaded applications are listed under Installed Applications together with information about the application's version, vendor, status (running or not running) and license information.

To start and stop an application, click the **Start** and **Stop** buttons.

To remove an uploaded application, select the application and click **Remove**.

Click **Log** to generate a log of the application happenings. The log is helpful when requesting support from the application's vendor.

For information on how to use the uploaded application, please refer to the documentation of the application package.

Note:

It is recommended to run one application at a time. Avoid running applications when motion detection is active.

Events

An **event** or **Event Type** triggers actions when activated. An event type is a set of parameters that defines the actions. A common event type is an alarm that causes the camera to upload images. Many event types require an **Event Server**, to receive uploaded images.

This section describes how to configure the camera to perform certain actions when events occur.

Definitions

Event type	A set of parameters describing how and when the camera performs certain actions
Triggered Event - see page 27	An event that is started by some sort of signal, for example, an external device such as a door switch, motion detection, or system event.
Scheduled Event - see page 28	An event that runs during pre-programmed time period(s).
Action	This occurs when the event runs, for example, uploading of images to an FTP server, or email notification.

Event Servers

Event Servers are used to receive uploaded image files and/or notification messages. To set up Event Server connections in your camera, go to **Setup > Events > Event Servers** and enter the required information for the required server type.

Server type	Purpose	Information required
FTP Server	• Receives uploaded images	• Descriptive name • Network address (IP address or host name) • User name and password
HTTP Server	• Receives notification messages • Receives uploaded images	• Descriptive name of your choice • URL (IP address or host name) • User name and password • Proxy settings
TCP Server	• Receives notification messages	• Descriptive name • Network address (IP address or host name) • Port number

For details on each setting, see the online help available from each web page.

When the setup is complete, the connection can be tested by clicking the **Test** button (the connection test takes approximately 10 seconds).

Event Types

An **Event Type** describes how and when the camera is to perform certain actions.

Example: If a person or object passes in front of the camera and an event has been configured to detect and respond to motion, the camera can record and save images to an FTP server, and can send a notification e-mail to an e-mail address. Images can be sent as e-mail attachments.

Triggered Event

A triggered event can be activated (triggered) by:

- Input ports – A signal from an alarm device connected to an input port
- Manual trigger – The event is activated manually using the manual trigger button on the Live View page or through the VAPIX® Application Programming Interface
- Application trigger – Using an uploaded application, see page 25
- Motion detection – Detected movement in a configured motion detection window
- Audio – When the sound level rises above or falls below the alarm level (configured under **Video & Audio > Audio Settings**, see page 19.
- On boot – On restart, for example after power loss
- Pan Tilt Zoom – When the camera stops at a preset position
- Camera tampering – If the camera is repositioned or the lens is covered, see page 28
- Disk full – When the SD memory card has less than 1 MB free memory
- Fan malfunction

How to set up a triggered event

The following example describes how to configure a triggered event to upload images when motion is detected.

1. Go to **Setup > Events > Event Types.**
2. Click **Add triggered...** to open the **Triggered Event Type Setup** page.
3. Enter a descriptive **Name** for the event.
4. Set the **Priority** - High, Normal or Low (see the online help).
5. Set the minimum time interval between triggers to avoid repeated triggers for the same event.
6. Set the **Respond to Trigger...** parameters to define when the event is active, for example, after office hours.
7. From the **Triggered by...** drop-down list, select Motion detection. Select a motion detection window and specify if the event is to be triggered when motion starts or stops.
8. Set the **When Triggered...** parameters, that is, define what the camera should do when motion is detected. To upload images, select **Save stream** and enter the required information, see *Save stream*, on page 27**.**
9. Click **OK** to save the event in the Event Types list.

Please see the online help for descriptions of each available option.

Note:

Up to 10 event types can be configured in the camera, and up to three of these can be configured to upload images. File names can be formatted according to specific requirements. See File Naming & Date/Time Formats online help.

Save stream

To upload images to an FTP or HTTP server, save the video stream to the local storage disk, or to send images by email, check the **Save stream** box.

Image frequency – Set the image frequency to a desired frame rate.

Pre- and post-trigger buffers

This function is very useful when checking to see what happened immediately before and/or after a trigger, for example, 20 seconds before and after a door was opened. All uploaded images are JPEG images.

Include pre-trigger buffer – Images stored internally in the server from the time immediately preceding the trigger. Check the box to enable the pre-trigger buffer and specify the buffer length in seconds, minutes or hours.

Include post-trigger buffer – Contains images from the time immediately after the trigger. The post-trigger buffer is configured in the same way as the pre-trigger buffer.

Notes:

- Pre-trigger and post-trigger buffers will be lost if the connection to the event server fails
- The maximum length of the pre-/post-buffer depends on the video image size and selected frame rate
- If the pre- or post-buffer is too large for the camera's internal memory, the buffer length is reduced. If this occurs, an entry is created in the unit's log file

Continue image upload (unbuffered) – Upload video images for a fixed length of time or for as long as the trigger is active. The frame rate will be the best possible, but might not be as high as specified under image frequency, especially if uploading via a slow connection.

Select type – Upload images to an FTP or HTTP server, send images by email or save the video stream to the local storage disk.

Create folder – Images uploaded to FTP and HTTP servers can be saved to designated folders. Folders can for example be named using the current date and time, see File Naming & Date/Time Formats in the online help.

Base file name – Used to name all uploaded images. Add a suffix or use your own file format to give the images unique names, see File Naming & Date/Time Formats in the online help.

Use stream profile – Select the stream profile to upload, send as email or save to the local disk.

Scheduled Event

A **Scheduled event** can be activated at preset times, in a repeating pattern on selected weekdays.

How to set up a scheduled event:

The following example describes how to set up a scheduled event.

1. Go to **Setup > Events > Event Types.**
2. Click **Add scheduled...** to open the **Scheduled Event Type Setup** page.
3. Enter a descriptive **Name** for the event, such as 'Scheduled e-mail upload'.
4. Set the **Priority** (High, Normal or Low).
5. Set the **Activation Time** parameters (24h clock) for the event. For example, select **Recurrence pattern** and let the event start on Sundays at 13.00 with a duration of 12 hours.
6. Set the **When Activated...** parameters, that is, define what the camera should do when the event is active. To upload images, select **Save stream** and enter the required information.See *Save stream*, on page 27.
7. Click **OK** to save the Event in the Event Types list.

Please see the online help for descriptions of each available option.

Camera tampering

The network camera can generate an alarm whenever the camera is repositioned, or when the lens is covered, sprayed, or severely defocused.

The camera tampering settings are configured on the **Events > Camera Tampering** page as described below. For the camera to send an alarm you must also create an event, see *How to set up a triggered event*, on page 27.

Camera Tampering Settings

The **Minimum duration** parameter sets the minimum tampering period, that is an alarm will not be triggered until this period has elapsed, even if the tampering conditions are otherwise met. This can help prevent false alarms for known conditions that affect the image.

Motion Detection

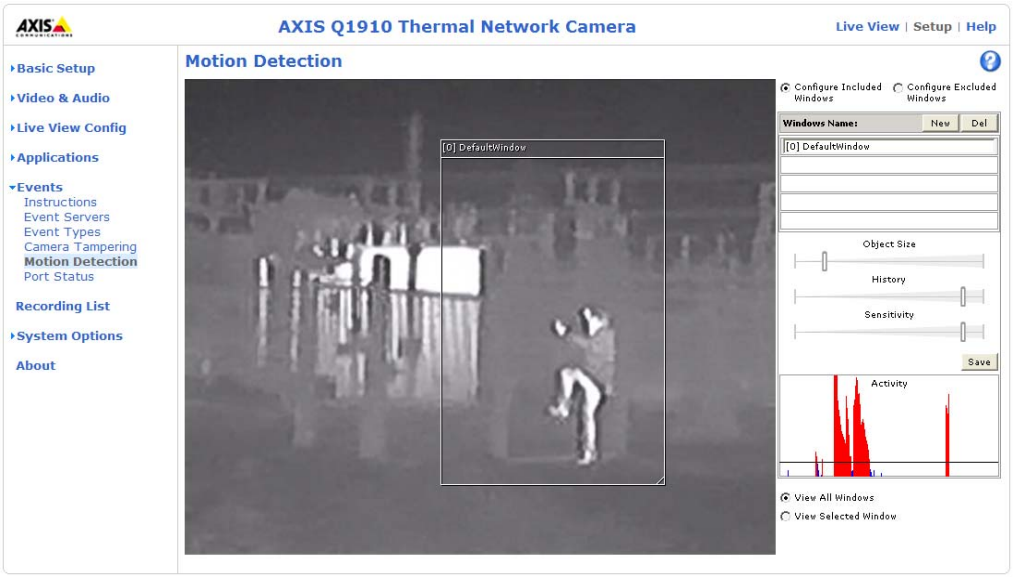
Motion detection is used to generate an alarm whenever movement occurs (or stops) in the camera's field of view. A total of 10 Include and Exclude windows can be configured.

- **Included** windows target specific areas within the whole image
- **Excluded** windows define areas within an Include window that should be ignored (areas outside Include windows are automatically ignored)

Once configured, motion detection appears in the list of available triggers, for triggering events. See *How to set up a triggered event*, on page 27.

Note:

Using the motion detection feature may decrease the camera's overall performance.



Set up a motion detection window

The following example describes how to configure the camera for motion detection.

1. Go to **Setup > Events > Motion Detection.**
2. Create a new motion detection window:
   a) Using AXIS Media Control (Internet Explorer): Select Configure **Included Windows** and click New. Select the new window in the list of windows and enter a descriptive name.
   b) Using the Java applet: Click Add Window. Select the Include radio button and enter a descriptive name in the field.
3. Adjust the size (drag the bottom right-hand corner) and position (click on the text at the top and drag to the desired position) of the active window.
4. Adjust the **Object Size**, **History** and **Sensitivity** profile sliders (see table below for details). Any detected motion within an active window is then indicated by red peaks in the **Activity** window (the active window has a red frame).
5. Click **Save**.

> To exclude parts of the Include window, select the **Exclude** option and position the Exclude window as required, within the Include window.

To delete an Include or Exclude window:

a) Using AXIS Media Control (Internet Explorer): Select the window and click **Del**.
b) Using the Java applet: Select the window and click on the cross in the upper right corner.

Please see the online help for descriptions of each available option.

	Object Size	History	Sensitivity
High level	Only very large objects trigger motion detection	An object that appears in the region will trigger the motion detection for a long period	Ordinary colored objects on ordinary backgrounds will trigger the motion detection
Low level	Even very small objects trigger motion detection	An object that appears in the region will trigger motion detection for only a very short period	Only very bright objects on a dark background trigger motion detection
Default value	Low	High	High

Examples:

- Avoid triggering on small objects by setting the **object size** level to high.
- Use several small Motion Detection windows rather than one large window, if triggers on small movements or objects are desired.
- To reduce the number of triggers if there is a lot of movement during a short period of time, select a high **history** level.

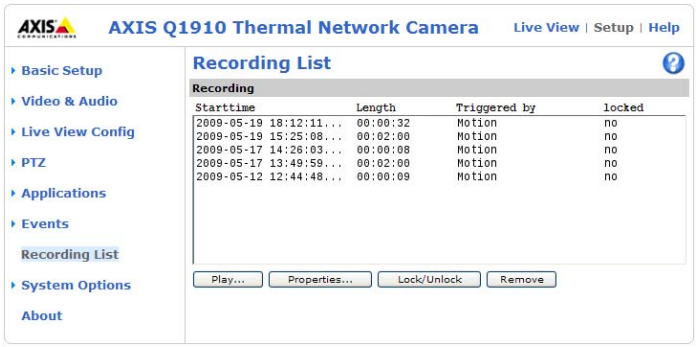
Port Status

Under **Setup > Events > Port Status** there is a list showing the status for the camera's input and output. This is for the benefit of **Operators** who have no access to the System Options section.

Example: If the Normal state for a push button connected to an input is set to **Open circuit -** as long as the button is not pushed, the state is **inactive**. If the button is pushed, the state of the input changes to **active**.

Recording List

The Recording List window contains a list of recordings made to the memory card. It shows each recording's start time, length, the event type used to start the recording, and indicates if the recording is locked so that it can neither be deleted nor recorded over.



To view a recording, select it from the list and click the **Play...** button.

For detailed recording and video information, select an individual recording from the list and click the **Properties...** button.

Use the **Lock/Unlock** button to define whether a recording can be removed or recorded over, or if the recording is important and needs to be saved for future use. Locking the recording can help prevent its accidental removal.

The **Remove** button is used to delete unlocked recordings.

Recordings are made to the SD memory card once an event has been set up on under **Setup > Event Types > Add triggered.../Add scheduled> Save stream > Select type.** Select Local Storage from the drop-down list.

See **Setup > System Options > Storage > SD Card** to connect, format and monitor the status and available recording space of the SD memory card.

Notes:

- Audio recordings cannot be saved to the SD memory card.
- The SD memory card is optional and not included in the product.
- To play recordings in Windows Media Player, download and install AXIS Matroska File Splitter from www.axis.com/techsup/software

System Options

Security

Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:

The **user list** displays the authorized users and user groups (levels):

Viewer	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

HTTP/RTSP Password Settings - Select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you recently upgraded the firmware and the existing clients do support encryption, but need to log in again, and be configured to use this functionality.

User Settings

- Check the checkbox to enable **anonymous viewer login** to allow any viewer direct access to the Live View page.
- Check the checkbox to enable **anonymous PTZ control login** to allow anonymous users to join a queue for gaining control of the PTZ controls.
- **Enable Basic Setup** - before using the network camera, there are certain settings that should be made, most of which require Administrator access privileges. To quickly access these settings, use the Basic Setup in the menu. All settings are also available from the standard setup links in the menu. Basic Setup is enabled by default but can be disabled and removed from the menu.

IP Address Filter

Enable IP Address Filtering to allow or deny access to the network camera**.** Once enabled, the IP addresses in the list are allowed or denied access according to the choice made in the drop-down list **Allow/Deny the following IP addresses.**

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses). The users from these IP addresses need to be specified in the user list with the appropriate access rights. This is done from **Setup > System Options > Security > Users**.

HTTPS

The network camera supports encrypted browsing using HTTPS.

A **self-signed certificate** can be used until a Certificate Authority-issued certificate has been obtained. Click **Create self-signed certificate** to install a self-signed certificate. Although self-signed certificates are free and offer some protection, true security is only implemented after the installation of a signed certificate issued by a certificate authority.

A signed certificate can be obtained from an issuing Certificate Authority by clicking the **Create Certificate Request** button. When the signed certificate is returned, click the **Install signed certificate** button to import the certificate. The properties of any certificate request currently resident in the camera or installed can also be viewed by clicking the **Properties...** button. The HTTPS Connection Policy must also be set in the drop-down lists to enable HTTPS in the camera.

For more information, refer to the online help .

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Admission Control. It provides authentication to devices attached to a network port (wired or wireless), establishing a point-to-point connection, or, if authentication fails, preventing access on that port. 802.1X is based on EAP (Extensible Authentication Protocol).

In a 802.1X enabled network switch, clients equipped with the correct software can be authenticated and allowed or denied network access at the Ethernet level.

Clients and servers in an IEEE 802.1X network may need to authenticate each other by some means. In Axis implementation this is done with the help of digital certificates provided by a **Certification Authority**. These are then validated by a third-party entity, such as a **RADIUS server**, examples of which are Free Radius and Microsoft Internet Authentication Service. To perform the authentication, the RADIUS server uses various EAP methods/protocols, of which there are many. The one used in Axis implementation is EAPOL using EAP-TLS (EAP-Transport Layer Security).

The Axis network video device presents its certificate to the network switch, which in turn forwards this to the RADIUS server. The RADIUS server validates or rejects the certificate and responds to the switch, and sends its own certificate to the client for validation. The switch then allows or denies network access accordingly, on a preconfigured port.

Certificates

CA Certificate – This certificate is created by the Certification Authority for the purpose of validating itself, so the camera needs this certificate to check the server's identity. Provide the path to the certificate directly, or use the **Browse...** button to locate it. Then click the **Upload** button. To remove a certificate, click the **Remove** button.

Client certificate/private key – The camera must also authenticate itself, using a client certificate and a private key. Provide the path to the certificate in the first field, or use the **Browse...** button to locate it. Then click the **Upload** button. To remove a certificate, click the **Remove** button.

Alternatively, it may be possible to upload the certificate and key in one combined file, (e.g. a PFX file or PEM file). Provide the path to the file, or use the **Browse...** button to locate it. Click **Upload** to load the file. To remove a certificate and key, click the **Remove** button.

Settings

EAPOL version – Select the EAPOL version (1 or 2) as used in your network switch.

EAP identity – Enter the user identity associated with your certificate. A maximum of 16 characters can be used.

Private key password – Enter the password (maximum 16 characters) for your user identity.

Enable IEEE 802.1X – Check the provided box to enable the IEEE 802.1X protocol.

Audio Support

Enable audio support – Allow clients to retrieve audio streams from the camera. See also *Audio Settings,* on page 19 for information on how to configure the audio settings.

Note:

This parameter will enable/disable all audio functionality in the camera, even in configured events and profiles.

Date & Time

Current Server Time
Displays the current date and time (24h clock). The time can be displayed in 12h clock format in the overlay (see below).

New Server Time
Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the **Automatically adjust for daylight saving time changes**.

Note:

The time zone setting only applies when the device's time is synchronized with an NTP server.

From the **Time Mode** section, select the preferred method to use for setting the time:

- **Synchronize with computer time** - Sets the time from the clock on your computer.
- **Synchronize with NTP Server** - The camera will obtain the time from an NTP server
- **Set manually** - This option allows you to manually set the time and date.

Note:

If using a host name for the NTP server, a DNS server must be configured under **TCP/IP** settings. See *Basic TCP/IP Settings*, below.

Date & Time Format Used in Images - Specify the formats for the date and time (12h or 24h) displayed in the video streams. Use the predefined formats or use your own custom date and time formats. See **Advanced File Naming & Date/Time Formats** in the online help for information on how to create your own date and time formats.

Network

Basic TCP/IP Settings

The network camera supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the network camera receives an IP address according to the configuration in the network router. There are also options for using AVHS (AXIS Video Hosting System) and AXIS Internet Dynamic DNS Service. For more information on setting the IP address, please see the online help.

Network Settings

Click the **View** button for an overview of the IP configuration of the network camera.

IPv4 Address Configuration

Check the box to enable IPv4.

Obtain IP address via DHCP – Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

Note:

DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the camera by name (host name). If DHCP is enabled and you cannot access the unit, run AXIS IP Utility to search the network for connected Axis products or reset the network camera to factory default settings and then perform the installation again.

Use the following IP address – To use a static IP address for the network camera, check the radio button and then make the following settings:

- IP address – Specify a unique IP address for your camera. (To check if the IP address you intend to use is available or not, click the Test button)
- Subnet mask – Specify the mask for the subnet the camera is located on
- Default router – Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

IPv6 Address Configuration

Check the box to enable IPv6. Other settings for IPv6 are configured in the network router.

Services

Enable ARP/Ping setting of IP address – The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service. Leave disabled to prevent unintentional resetting of the IP address.

Notes:

- The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set. In order to reset the IP address, the camera must be restarted to activate ARP/Ping for an additional two minutes.
- Pinging the unit is still possible when this service is disabled.

AXIS Video Hosting System (AVHS)

AVHS used in conjunction with an AVHS service provides easy and secure Internet access to live and recorded video accessible from any location. For more information and help to find a local AVHS Service Provider go to www.axis.com/products/avhs

Enable AVHS – Enabled by default; if AVHS is not to be used this option can be disabled.

One-click enabled – Press the camera's control button (see *Hardware overview,* on page 5) to connect to an AVHS service over the Internet. Once registered, **Always** will be enabled and the camera will stay connected to the AVHS service. If the camera is not registered within 24 hours from when the button was pressed, the camera will disconnect from the AVHS service.

Always – The camera will constantly attempt to connect to the AVHS service over the Internet; once registered the camera will stay connected to the service. This option can be used when the camera is already installed and it is not convenient to use the one-click installation.

AXIS Internet Dynamic DNS Service

Enable this option to use AXIS Internet Dynamic DNS Service to assign a host name for easy access to your network camera.

Click **Settings...** to register the camera with AXIS Internet Dynamic DNS Service, or to modify the existing settings (requires access to the Internet). The domain name currently registered at the Axis Internet Dynamic DNS Service for your product can at any time be removed.

For more information, please refer to www.axiscam.net and to the online help.

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses on your network.

Obtain DNS server address via DHCP - Automatically use the DNS server settings provided by the DHCP server. Click the **View** button to see the current settings.

Use the following DNS server address - Enter the desired DNS server by specifying the following:

- **Domain name** - Enter the domain(s) to search for the host name used by the network camera. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, for example, **myserver** is the host name in the Fully Qualified Domain Name **myserver.mycompany.com** where mycompany.com is the Domain name.
- **DNS servers** - Enter the IP addresses of the primary, and secondary DNS servers.
  Note: This is not mandatory with regard to secondary DNS servers.

NTP Configuration

Obtain NTP server address via DHCP - Check this radio button to automatically look up and use the NTP server settings as provided by DHCP. Click the **View** button to see the current settings.

Use the following NTP server address – To create manual settings, check this radio button and enter the host name or IP address of the NTP server.

Host Name Configuration

The network camera can be accessed using a host name, instead of an IP address. The host name is usually the same as the assigned DNS Name.

Link-Local IPv4 Address

This is enabled by default and assigns the network camera an additional IP address for use with UPnP™. The camera can have both a Link-Local IP and a static/DHCP-supplied IP address at the same time - these will not affect each other.

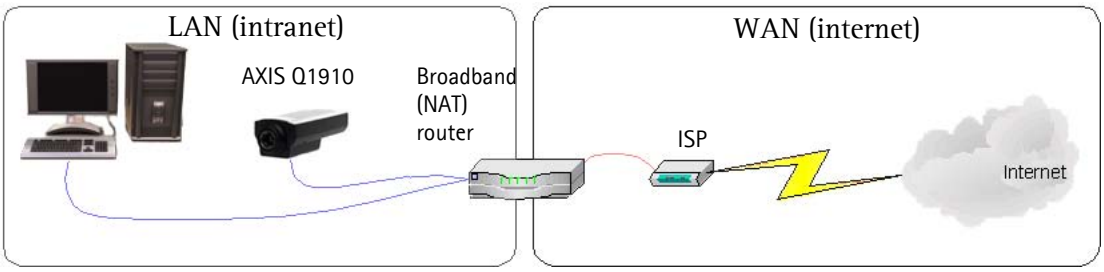
HTTP and HTTPS

The default HTTP/HTTPS port numbers (80 and 443 respectively) can be changed to any port within the range 1024-65535. This is useful for simple security port mapping, for example.

NAT traversal (port mapping) for IPv4

A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your network camera is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the camera.



Notes:

- For NAT traversal to work, this must be supported by the broadband router.The router must also support UPnP™**.**
- The broadband router has many different names: "NAT router", "Network router", Internet Gateway", "Broadband sharing device" or "Home firewall" but the essential purpose of the device is the same.

Enable/Disable - When enabled, the network camera attempts to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the camera (see **System Options > Network > UPnP**).

Use manually selected NAT router - Select this option to manually select a NAT router and enter the IP address for the router in the field provided.

If a router is not manually specified, the network camera automatically searches for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port - Select this option to manually define an external HTTP port. Enter the port number in the field provided. If no port is entered here a port number is automatically selected when NAT traversal is enabled.

Notes:

- An alternative HTTP port can be used/be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this enter a new port number and click Save.

FTP

The FTP server running in the network camera enables the upload of new firmware, and user applications. Check the box to enable the service.

RTSP

The RTSP protocol allows a connecting client to start an H.264 stream. Check the box to enable the server and enter the RTSP port number to use. The default setting is 554. Note that H.264 video streams will not be available if this service is not enabled.

SOCKS

SOCKS is a networking proxy protocol. The network camera can be configured to use a SOCKS server to reach networks on the other side of a firewall/proxy server. This functionality is useful if the network camera is located on a local network behind a firewall, and notifications, uploads, alarms, and such need to be sent to a destination outside the local network (such as the Internet). See the online help for more information.

QoS (Quality of Service)

Quality of Service (QoS) guarantees a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses. The main benefits of a QoS-aware network can be summarized as:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

The QoS in Axis network video products marks the data packets for various types of network traffic originating from the product. This makes it possible for network routers and switches to reserve a fixed amount of bandwidth for these types of traffic. The network camera marks the following types of traffic:

- video
- audio
- event/alarm
- management network traffic

QoS Settings - For each type of network traffic supported by your Axis network video product, enter a DSCP (Differentiated Services Codepoint) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch the type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

For more information on Quality of Service, please see Axis support web at www.axis.com/techsup

SMTP (email)

Enter the host names (or IP addresses) and port numbers for your primary and secondary mail servers in the fields provided, to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.

If your mail server requires authentication, check the box for **Use authentication to log in to this server** and enter the necessary information. See the online help for more information.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

Depending on the level of security required, select the version of SNMP to use.

SNMP v1/v2

Select either SNMP v1 that includes no security, or SNMP v2c that uses very simple security.

The community name can be specified as a password for read or read/write access to all supported SNMP objects. The community is the group of network devices using SNMP. The default password for the **Read Community** is **public** and the default password for the **Write community** is **write**.

Traps for SNMP v1/v2

Traps are used by the camera to send messages to a management system for important events or status changes.

If **Enable traps** is selected, enter the email address where the trap message is to be sent as well as the **Trap community** that should receive the message.

There are four types of traps available for the network camera:

- Cold start
- Warm start
- Link up
- Authentication failed

SNMP v3

SNMP v3 provides encryption and secure passwords. HTTPS must be enabled. To use traps with SNMP v3 an SNMP v3 management application is required.

If the **Enable SNMP v3** option is selected, provide the Initial user password. Note that the initial password is activated only when HTTPS is enabled and can only be set once.

If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

When the SNMP configuration is ready, click **Save** to use the new settings. Click **Reset** to return to the default values.

UPnP™

The network camera includes support for UPnP™. UPnP™ is enabled by default, and the network camera then is automatically detected by operating systems and clients that support this protocol.

RTP/H.264

These settings are the port range, IP address, port number (video and audio), and Time-To-Live value to use for the video stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams. For more information, please see the online help .

Bonjour

The network camera includes support for Bonjour. When enabled, the camera is automatically detected by operating systems and clients that support this protocol.

Storage

SD Card

The **Disk Management** window is used to set up and manage local storage. It is used to connect memory cards for recording video, monitoring a disk's status, enabling automatic cleanup and preventing the memory card from being overwritten.

Storage Device

Storage device is used to identify and monitor the status of the SD card. it shows the size of the memory card and how much free space is available for storage. It is also used to mount and format SD cards for local storage.

Device Settings

Device settings is used to configure removal of recorded video. Automatic disk cleanup can be enabled and set up according to a schedule, and an SD card can be locked to prevent storage removal.

Ports & Devices

I/O Ports

The network camera has two configurable input/output ports for connection of external devices. Select the port direction (**Input** or **Output**) from the drop-down list. The ports can be given descriptive names and their **Normal state** and be configured as Open circuit or Grounded circuit.

See *Unit connectors*, on page 6, for information on how to connect external devices.

COM Port

This page contains settings for the RS-485/RS-422 serial interface. To enable support for a pan/tilt motor connected to the camera's RS-485/422 port, select **Pan Tilt Zoom** from the **Usage** drop-down list and click **Save**.

See also *PTZ (Pan Tilt Zoom)*, on page 23.

See *Unit connectors*, on page 6, for wiring information.

LED Settings

The Status indicator LED on the camera can be set to flash at a configurable interval (or to not light up at all) when the unit is accessed. For a listing of all LED behavior, see page 8, or the online help.

The LED does not flash when the stream is retrieved using H.264 multicast.

Maintenance

Restart – The camera is restarted without changing any settings.

Restore – The camera is restarted and most settings are reset to factory default values. The settings that do not reset are:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the system time
- the IEEE 802.1x settings

Default – The default button should be used with caution. Click this returns the camera's setting to the factory default values (including the IP address).

Upgrade Server – See *Upgrading the firmware*, on page 43.

Support

Support Overview

The **Support Overview** page provides valuable information on troubleshooting and contact information, should you require technical assistance.

System Overview

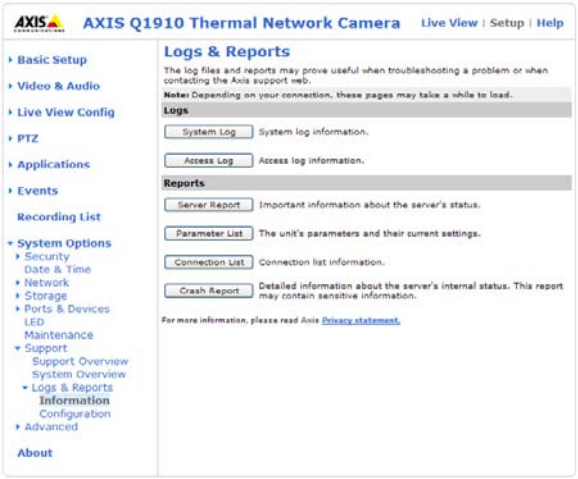
System Overview provides an overview of the camera's status and settings. Information that can be found here includes the camera's firmware version, IP address, security, event and image settings and recent log items. Many of the captions are also links to the proper **Setup page** to conveniently make adjustments in the camera's settings.

Logs & Reports

When contacting Axis support, please be sure to provide a valid Server Report with your query. The Access Log is automatically included in the server report.

Information

The **Server Report** and **Parameter List** may prove useful when troubleshooting a problem or when contacting Axis support.



- **System Log** - Provides information about system events.
- **Access Log** - By default, the Access Log lists all failed attempts to access the camera but can be configured to list all connections to the camera, whether successful or not. Go to **Support > Logs & Reports > Configuration** and select the desired level of information from the list. See below for more information. The Access Log is useful for various purposes such as tracking all access to the camera, system analysis and troubleshooting.
- **Server Report** - Provides information about the server status and should always be included when requesting support.
- **Parameter List** - Shows the unit's parameters and their current settings.
- **Connection List** - Lists all clients that are currently accessing video and audio. It is also used for system analysis and troubleshooting.
- **Crash Report** – Generates an archive with debugging information. Note that the report takes several minutes to generate.

Configuration

From the drop-down lists, select the level of information to be added to the **System Log** and **Access Log** files and the permitted size of the log files.

The default information level for the Access Log is set to Critical & Warnings, i.e. failed connections. However, in an error situation and when requesting support, set it to the highest information level - Critical & Warnings & Info.

For the Log Level for Email, select from the drop-down list the level of information to send as email and enter the destination email address.

Advanced

Scripting

Scripting is an advanced function that enables you to customize and use scripts. This function is a very powerful tool.

Caution!

Improper use may cause unexpected behavior or even cause loss of contact with the unit. If a script does cause problems, reset the unit to its factory default settings. A backup file may be of use to return the unit to its latest configuration.

Axis strongly recommends that you do not use this function unless you understand the consequences. Note that Axis support does not provide assistance for problems with customized scripts.

For more information, please visit the Developer pages at www.axis.com/developer

File Upload

Files (e.g. web pages and images) can be uploaded to the network camera and used as custom settings. Uploaded files are accessed via http://<ip address>/local/<user>/<file name> where <user> is the selected user access group (viewer, operator or administrator) for the uploaded file.

Plain Config

Plain Config is for the advanced user with experience of Axis network camera configuration. All parameters can be set and modified from this page. Help is available from the standard help pages.

About

Here you can find basic information about your network camera. You can also view third party software licenses.

Resetting to the factory default settings

To reset the camera to the original factory default settings, go to the **System Options > Maintenance** web page (as described in *Maintenance*, on page 39) or use the **Control button** on the side of the camera (see page 6) as described below:

Using the Control Button

To reset the camera to the factory default settings using the Control Button:

1. Disconnect power from the camera. If PoE is used, disconnect the network cable.
2. Press and hold the Control button while reconnecting power.
3. Keep the Control button pressed until the **Status Indicator** color changes to amber (this may take up to 15 seconds).
4. Release the Control button. When the Status Indicator changes to green (which may take up to 1 minute), the process is complete and the camera has been reset. The unit now has the default IP address 192.168.0.90
5. Re-assign the IP address, for instructions see the Installation Guide supplied with the camera.

Troubleshooting

Checking the firmware

Firmware is software that determines the functionality of network cameras. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in your camera is displayed on the page **Setup > Basic Setup** or under **About.**

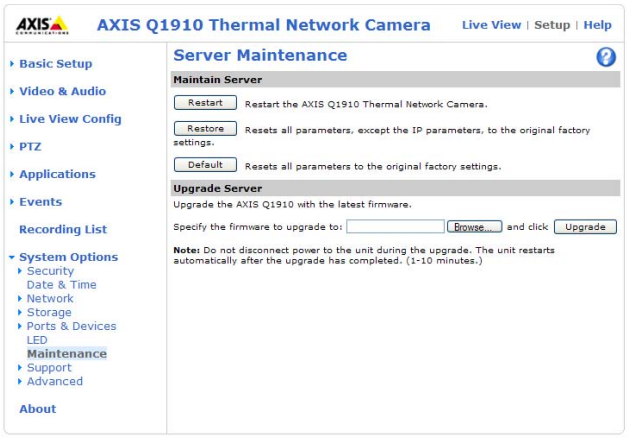
Upgrading the firmware

When you upgrade your camera with the latest firmware from Axis web site, your camera receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release, before updating the firmware.

Note:

Preconfigured and customized settings are saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications.

1. Save the firmware file to your computer. The latest version of the firmware is available free of charge from Axis web site at **www.axis.com/techsup**
2. Go to **Setup > System Options > Maintenance** in the camera's web pages.
3. In the **Upgrade Server** section, browse to the desired firmware file on your computer. Click **Upgrade**.



Notes:

- After starting the upgrade process, always wait at least 5-10 minutes before restarting the camera, even if you suspect the upgrade has failed.
- Your dealer reserves the right to charge for any repair attributable to faulty upgrading by the user.
- AXIS Camera Management can be used for multiple upgrades. Please see Axis web site at www.axis.com for more information.

Emergency Recovery Procedure

If power or the network connection to the camera is lost during the upgrade, the process fails and the unit becomes unresponsive. A flashing red Status LED indicates a failed upgrade. To recover the unit, follow the steps below. The serial number is found on the label attached to the bottom of the camera.

1. **UNIX/Linux** - From the command line, type the following:
   arp -s <IP address of camera> <serial number> temp
   ping -s 408 <IP address of camera>

   Windows - From a command/DOS prompt, type the following:
   arp -s <IP address of camera> <serial number>
   ping -l 408 -t <IP address of camera>
2. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to stop Ping.
3. Open a browser and type in the camera's IP address. In the page that appears, use the **Browse** button to select the upgrade file to use, for example, AXIS_Q1910.bin. Then click the Load button to restart the upgrade process.
4. After the upgrade is complete (1-10 minutes), the unit automatically restarts and shows a steady green on the Power and Status LEDs and flashing green or amber on the Network LED.
5. Reinstall the camera, referring to the installation guide.

If the emergency recovery procedure does not get the camera up and running again, please contact Axis support at www.axis.com/techsup/

Axis Support

If you contact Axis support, please help us resolve your problem expediently by providing a **Server Report** and a detailed description of the problem.

The Server Report contains important information about the server and its software, as well as a list of the current parameters. The Access Log is also included in the Server Report. Go to **Setup > System Options > Support > Support Overview** to generate a Server Report.

Symptoms, possible causes, and remedial action

Problems setting the IP address	
When using ARP/Ping	Try the installation again. The IP address must be set within two minutes after power has been applied to the camera. Ensure the Ping length is set to 408. See the Installation Guide.
The camera is located on a different subnet	If the IP address intended for the camera and the IP address of your computer are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an appropriate IP address.
The IP address is being used by another device	Disconnect the camera from the network. Run the Ping command. (In a Command/DOS window, type **ping** and the **IP address** of the unit). If you receive: **Reply from <IP address>: bytes = 32; time = 10 ms.....** - this means that the IP address may already be in use by another device on your network. You must obtain a new IP address and reinstall the unit. If you see: **Request timed out** - this means that the IP address is available for use with your camera. In this case, check all cabling and reinstall the unit.
Possible IP address conflict with another device on the same subnet	The static IP address in the camera is used before the DHCP server sets a a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the camera. To avoid this, set the static IP address to 0.0.0.0.
The camera cannot be accessed from a browser	
The IP address has been changed by DHCP	If the camera and client are on the same network, Run AXIS IP Utility to locate the camera. Identify the camera using its model or serial number Alternatively: 1) Move the camera to an isolated network or to one with no DHCP or BOOTP server. Set the IP address again, using the AXIS IP Utility (see the Installation Guide) or the ARP/Ping commands. 2) Access the unit and disable DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit now has a dynamic IP address, but will notify you if the address changes.
Other networking problems	Test the network cable by connecting it to another network device, then Ping that device from your workstation. See instructions above.
Camera is accessible locally, but not externally	
Broadband router configuration	To configure your broadband router to allow incoming data traffic to the camera, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the camera. This is enabled from **Setup > System Options > Network > TCP/IP Advanced**.
Firewall protection	Check the Internet firewall with your system administrator.
Default routers required	Check if you need to configure the default router settings.
Problems with the H.264 format	
No H.264 displayed in the client	Check that the correct network interface is selected in the AMC control panel applet (streaming tab).
	Check that the relevant H.264 connection methods are enabled in the AMC control panel applet (streaming tab).
	In the AMC control applet, select the H.264 tab and click the button Set to default H.264 decoder.
No multicast H.264 displayed in the client	Check with your network administrator that the multicast addresses used by the camera are valid for your network.
	Check with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL (Time To Live) value may need to be increased.

Poor rendering of H.264 images	Color depth set incorrectly on clients. Set to 16-bit or 32-bit color.
	If text overlays are blurred, or if there are other rendering problems, you may need to enable Advanced Video Rendering from the H.264 tab in the AMC control panel applet.
	Ensure that your graphics card is using the latest device driver. The latest drivers can usually be downloaded from the manufacturer's web site.
Image degeneration	Decrease the GOV length, see the online help for more information.
The Power indicator is not constantly lit	
Faulty power supply	Check your power supply.
The Status and Network indicator LEDs are flashing red rapidly	
Hardware failure	Contact your Axis dealer.
The Status indicator LED is flashing red and the camera is inaccessible	
A firmware upgrade has been interrupted or the firmware has otherwise been damaged	See the *Emergency Recovery Procedure* above.
No images displayed on web page	
Problem with AMC. (*Internet Explorer only*)	To enable the updating of video images in Microsoft Internet Explorer, set your browser to allow ActiveX controls. Also, make sure that AXIS Media Control (AMC) component is installed on your workstation.
Installation of additional ActiveX component restricted or prohibited	Configure your camera to use a Java applet for updating the video images under **Live View Config > Layout > Default Viewer** for Internet Explorer. See the online help for more information.
Video/Image problems, general	
Missing images in uploads	This can occur when trying to use a larger image buffer than is actually available. Try lowering the frame rate or the upload period.
Slow image update	Configuring pre-buffers, motion detection, high-resolution images, or high frame rates, will affect the performance of the camera.
Poor quality snapshot images	
Screen incorrectly configured on your workstation	In Display Properties, configure your screen to show at least 65000 colors, that is, at least 16-bit. Using only 16 or 256 colors will produce dithering artifacts in the image.
Overlay/Privacy mask is not displayed	
Incorrect size or location of overlay or privacy mask.	The overlay or privacy mask may have been positioned incorrectly or may be too large. Refer to **Overlay Image Requirements and Limitations** in the online help for more information.
Browser freezes	
Netscape 7.x or Mozilla 1.4 (or later) can sometimes freeze on a slow computer	Lower the image resolution.
Problems uploading files	
Limited space	There is only limited space available for the upload of your own files. Try deleting existing files to free up space.
Motion Detection triggers unexpectedly	
Changes in luminance	Motion detection is based on changes in luminance in the image. This means that if there are sudden changes in the lighting, motion detection may be triggered mistakenly. Lower the sensitivity setting to avoid problems with luminance.
No audio	
Incorrect setup	Check the sound card in the PC. Ensure that the mute button is not pressed and the volume settings are correct.
No audio or very poor audio quality	Check that the correct Audio Input source is selected under **Setup > Audio > Source**. Select Microphone for the internal microphone or for a connected external microphone. Select Line for a connected line in source.

Audio volume too low/high	
Volume settings incorrect	The volume of the microphone is either too high or too low. Change the volume for the microphone in the toolbar on the Live View page.
Poor audio quality	
CPU overloaded	Reduce the number of listeners and viewers and decrease the image resolution and compression.
Unsynchronized audio and video	It is recommended that the camera's time setting is synchronized with an NTP Server. This is enabled under **System Options > Date & Time**.
Distorted audio	Check that the correct Audio Input source is selected under **Setup > Audio Settings > Source**. Select Microphone for the internal microphone or for a connected external microphone. Select Line for a connected line in source.

For further assistance, please contact your reseller or see the support pages on Axis web site at www.axis.com/techsup

Technical Specifications

Function/group	Item	Specification
Camera	Models	• Indoor: AXIS Q1910 • Outdoor: AXIS Q1910-E
	Image sensor	Uncooled Micro bolometer 160x128 pixels
	Lens	f 13 mm: F1.25 Angle of view, horizontal: 17°
	Zoom	Digital zoom
	Detection range	At least 200 m (220 yards) for humans (1.8m x 0.5 m) At least 550 m (600 yards) for vehicles (2.3 m x 2.3 m)
	Sensitivity	NetD < 100 mK
Video	Video compression	• H.264 (MPEG-4 Part 10/AVC) Baseline profile • Motion JPEG
	Resolutions	Sensor is 160x128. Image can be scaled up to 720x576 (D1) and to standard VGA resolutions.
	Frame rate H.264	8.33 fps
	Frame rate Motion JPEG	8.33 fps
	Video streaming	• At least 5 streams in H.264 and Motion JPEG: simultaneous, individually configured streams in max. resolution at 8.33 fps • Controllable frame rate and bandwidth • VBR/CBR H.264
	Image settings	• Compression, brightness, exposure control, rotation, mirroring of images • Text and image overlay • Privacy mask • Palettes
Audio	Audio streaming	Two-way
	Audio compression	• AAC LC 8/16 kHz • G.711 PCM 8 kHz • G.726 ADPCM 8 kHz • Configurable bit rate
	Audio Input/Output	AXIS Q1910: Built-in microphone, external microphone or line input, line output AXIS Q1910-E: External microphone or line input, line output
Network	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, digest authentication, user access log
	Supported protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS*, QoS Layer 3 DiffServ, FTP, SMTP, Bonjour, UPnP, SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, etc. Wide range of PT heads supported (drivers available for download at www.axis.com *This product includes software developed by the Open SSL Project for use in the Open SSL Tool kit (www.openssl.org)
System Integration	Application Programming Interface	Open API for software integration, including ONVIF, specification available at www.onvif.org, as well as VAPIX® and AXIS Camera Application Platform, specifications available at www.axis.com
	Intelligent video	• Video motion detection, active tampering alarm, audio detection • Support for AXIS Camera Application Platform enabling installation of third-party applications.
	Alarm triggers	Intelligent video, temperature, external input, disk full

Function/group	Item	Specification
	Alarm events	• File upload via FTP, HTTP and email • Notification via email, HTTP and TCP • External output activation • Play audio clip • Video recording to local storage
	Video buffer	32 MB pre- and post alarm
	Video access from web browser	• Camera live view • Video recording to file (ASF) • Customizable HTML pages • Windows 7, Windows Vista, XP, 2000, Server 2003 • DirectX 9c or higher • For other operating systems and browers see www.axis.com/techsup
General	**Casing**	AXIS Q1910: Zinc chassis AXIS Q1910-E: IP66-rated aluminum casing with germanium window
	Processors and memory	• ARTPEC-3, 128 MB RAM, 128 MB Flash • Battery backed-up real-time clock
	Power	• Power over Ethernet IEEE 802.3af Class 3 • 8 – 20 V DC max 11.2 W • 20 - 24 V AC max 17.4 VA Power supply not included
	Connectors	• RJ-45 10BASE-T/100BASE-TX PoE, • Terminal block for power • Terminal block for two configurable inputs/outputs • 3.5 mm mic/line in, 3.5 mm line out • Terminal block for RS-485/RS-422 • Terminal block for AXIS Q1910-E heater
	Local Storage	SD/SDHC memory card slot (card not included)
	Operating conditions	AXIS Q1910: -40 °C to 50 °C (-40 °F to 122 °F), humidity 20-80% RH (non-condensing) AXIS Q1910-E: -40 °C to 50 °C (-40 °F to 122 °F), IP66
	Approvals	• EN 55022 Class B • EN 61000-3-2 • EN 61000-3-3 • EN 55024 • EN 61000-6-1 • EN 61000-6-2 • EN 60950-1 • FCC Part 15, Subpart B, Class B • VCCI, Class B ITE • C-tick AS/NZS CISPR 22 • ICES-003, Class B • IP66
	Dimensions (HxWxD)	AXIS Q1910: 58 x 79 x 186 mm (2.3" x 3.1" x 7.3") AXIS Q1910-E: 120 x 161 x 404 mm (4.7" x 6.3" x 15.9")
	Weight	AXIS Q1910: 990 g (2.18 lb) AXIS Q1910-E: 3520 g (7.76 lb)

Function/group	Item	Specification
	Included accessories	Connector kit, Installation Guide, Windows decoder 1-user license AXIS Q1910-E: wall mount bracket, 5 m (16 ft) Ethernet cable
	Video management software (not included)	• AXIS Camera Station - Video management software for viewing and recording up to 50 cameras • See www.axis.com/partner/adp_partners.htm for more software applications via partners
	Optional accessories	• Wall bracket accessories • Pan/tilt motor • Power supply • Multi-user decoder license pack

General performance considerations

When setting up your system, it is important to consider how various settings and situations will affect performance. Several factors affect the amount of bandwidth (the bit rate) required; the following factors are among the most important to consider:

- High image resolutions and/or lower compression levels result in larger images.
- Access by large numbers of Motion JPEG and/or unicast H.264 clients.
- Simultaneous viewing of different streams (resolution, compression, etc.) by different clients.
- Accessing both Motion JPEG and H.264 video streams simultaneously.
- Enabled motion detection.
- Heavy network utilization due to poor infrastructure.

Index

A
Action Buttons 11, 22
Active/Inactive 22
Alarm 7, 29
AMC 9
ARP/Ping 35
Audio 17
Audio input 19
Audio output 20
Audio Settings 19
AXIS Media Control 19

B
Backup 40
Bit Rate 17
Bonjour 9
Buffer Size 27

C
Camera tampering 28
Control Button 42

D
Date & Time 34
Default Viewer 21
DNS Configuration 35
DNS Server 35, 36
Domain Name 36

E
Emergency Recovery 43
Enable ARP/Ping 35
Event Servers 26
Events 25

F
Factory Default Settings 42
FTP Server 26

G
GOV Settings 17

H
H.264 16, 17
Half duplex 19
Host Name 36
HTTP Server 26
HTTPS 10, 32, 36

I
I/O Ports 39
IEEE 802.1X 33
Input 7
IP Address Filtering 32

L
Live View 11
Live View Config 21
Logs & Reports 40

M
Motion Detection 7, 29

N
NAT traversal 10, 36
Network Settings 34
NTP Server 34

O
Output 7
Output Buttons 22

P
Palette 16
Pinout - I/O connectors 7
Port Status 30
Ports & Devices 39
Preset Positions 23
Pulse 11, 22

Q
QuickTime 14, 21

R
Recording List 31
Recovery 43

S
Scheduled Event 26, 28
Security 32
Server Time 34
Snapshot button 11
SNMP 38
Support 40
System Options 32

T
TCP Server 26
TCP/IP Settings 34
Time Mode 34
Triggered Event 26
Troubleshooting 43

U
Upgrade Server 40
UPnP 36, 38
Users 32

V
Video Stream 16